TAMPEREEN TEKNILLINEN YLIOPISTO

MIKKO MÄKIPÄÄ

PILVIPALVELUIHIN LIITTYVÄT VIRTUALISOIDUT LÄHIVERKOT

Diplomityö

Tarkastaja: professori Jarmo Harju
Tarkastaja ja aihe hyväksytty
Tieto- ja sähkötekniikan tiedekunta-
neuvoston kokouksessa 15. tammi-
kuuta 2014

TIIVISTELMÄ

TAMPEREEN TEKNILLINEN YLIOPISTO
Tietotekniikan koulutusohjelma
MÄKIPÄÄ, MIKKO: Pilvipalveluihin liittyvät virtualisoidut lähiverkot
Diplomityö, 89 sivua
Huhtikuu 2014
Pääaine: Tietoliikenneverkot ja protokollat
Tarkastaja: professori Jarmo Harju
Avainsanat: cloud computing, Extensible Switch, Microsoft Hyper-V, Network virtualization, software-defined networking, SDN, VXLAN, virtualization, vSwitch, dvSwitch, vCloud, VMware

Pilvipalveluiden merkitys on kasvanut viime vuosina merkittävästi ja se jatkaa edelleen kasvuaan. Pilvipalveluita hyödyntävät niin suuret kuin pienetkin organisaatiot. Pilvipalveluissa ja varsinkin pilviympäristöissä virtualisointi on yksi tärkeimmistä asioista. Virtualisointi on aikaisemmin painottunut enemmänkin resurssien, kuten laskentatehon ja levytilan virtualisointiin, mutta yhä suurempiin ja hajautetumpiin pilviympäristöihin siirtyminen on luonut tarpeen myös verkon virtualisoinnille. Tämän ovat huomanneet myös suuret virtualisointijärjestelmiä tarjoavat yritykset, kuten VMware ja Microsoft. VMware ja Microsoft ovatkin toteuttaneet lähiverkon virtualisoinnin sekä eristetyssä pilvijärjestelmässä että fyysisen verkon yli, käyttämällä kuitenkin poikkeavia lähestymistapoja ratkaisuissaan.

Tämän työn tarkoituksena on tutkia pilvipalveluihin liittyviä virtualisoituja lähiverkkoja ja niiden komponentteja, tutustuttaa lukija SDN-konseptiin sekä vertailla eri valmistajien välillä olevia verkon virtualisoinnin vaihtoehtoja. Jotta työstä saatiin mahdollisimman kattava, valittiin tarkasteltavaksi kaksi suurinta kaupallista pilviympäristöjen valmistajaa, VMware ja Microsoft. Työssä haluttiin lisäksi todentaa pilvipalvelun redundanttisuuteen liittyviä ominaisuuksia lähiverkon kannalta, jotta nämä ominaisuudet eivät jäisi ainoastaan valmistajien myyntipuheiksi. Työ jakaantuu neljään osaan: pilvipalveluiden ja virtualisoinnin teoriaosuuteen, eri valmistajien kehittämien verkon virtualisointiratkaisujen toiminnallisuuksien tarkasteluun ja vertailuun, lähiverkon redundanttisuuden testaamiseen ja SDN-konseptin esittelyyn.

Tutkimus osoittaa, että suuret pilviympäristön valmistajat ovat kehittäneet virtualisoiduista verkon laitteista toiminnallisuudeltaan lähes vastaavia kuin fyysiset verkkolaitteet ovat. On kuitenkin huomionarvoista, että mainospuheissa usein toistettu yksinkertaisuus ei ole välttämättä totta itse toteutuksen kannalta, sillä ohjelmallisesti toteutetut ratkaisut vaativat useita erilaisia komponentteja, jotta ne toimisivat halutulla tavalla. Lisäksi hieman valmistajasta riippuen ratkaisut ovat edelleen hyvin sidottuja alla olevaan fyysiseen laitteistoon ja pilviympäristön valmistajaan, jolloin yksinkertaisesta ja palveluperusteisesta pilvipalvelusta saattaakin muodostua sen hankkijalle suuremmat investoinnit kuin annetaan ymmärtää. SDN-konseptin voidaan sanoa olevan näkökulma oikeaan suuntaan, sillä sen laajempi käyttöönotto ja hyväksyntä mahdollistaisivat laitevalmistajasta riippumattoman ratkaisun verkon virtualisoinnille.

ABSTRACT

TAMPERE UNIVERSITY OF TECHNOLOGY
Master's Degree Programme in Information Technology
MÄKIPÄÄ, MIKKO: Virtualized local area networks in cloud services
Master of Science Thesis, pages 89
April 2014
Major: Communication Networks and Protocols
Examiner: Professor Jarmo Harju
Keywords: cloud computing, Extensible Switch, Microsoft Hyper-V, Network virtualization, software-defined networking, SDN, VXLAN, virtualization, vSwitch, dvSwitch, vCloud, VMware

The market share of cloud computing systems in IT industry has grown significantly in recent years and it still keeps growing. Cloud computing systems are used by both small and big organizations. Virtualization is an important part of cloud computing systems and specifically of cloud environments. At first, virtualization was concentrated mainly on virtualization of resources like computing and storage but the growth and distribution of cloud environments have also created a need for network virtualization. This has also been noticed by big virtualization platform vendors like VMware and Microsoft. VMware and Microsoft have realized virtualization of local area networks both in isolated cloud environments and over the underlying physical network by different approaches.

This thesis studies local area networks and components of cloud environments, familiarizes the reader with the SDN concept and compares the alternatives of network virtualization between different cloud platform vendors. As the goal of the thesis was to be as inclusive as possible, two of the biggest cloud environment vendors, VMware and Microsoft were chosen to be compared. Also the redundancy of the cloud environments and networks was tested so that the promised features would not be introduced only in sales speeches of the two cloud environment vendors. The thesis is divided into four parts: theory of cloud computing and virtualization, study and comparison of network virtualization and its functionalities by different vendors, testing of local area network redundancy in cloud environment and introduction of the SDN concept.

The thesis concludes that big cloud environment vendors have developed virtualized networking devices to be at almost the same level of functionality as the physical networking devices are. It is still worth mentioning that simplicity, which is often used in sales documentation of vendors, is not always the case in real life use. That is because the programmability of networking devices requires a lot of different components to achieve full functionality in them. Also depending on the vendor, they are still very tied to the underlying physical devices and to the specific vendor of the cloud environment. This might cause the simple, service-oriented and cost-effective cloud service to be more costly to the user than it has been implied. It can be said that the SDN concept is a step in the right direction in network virtualization because, when accepted widely, it would remove the need for vendor-specific devices in underlay networks.

ALKUSANAT

Tämä on SSP Yhtiöt Oy:lle tehty diplomityö. Ohjaajina SSP Yhtiöt Oy:n puolesta toimivat Ville Isotalo ja Antti Hurme. Tampereen teknillisen yliopiston osalta työn ohjaajana toimi Professori Jarmo Harju. Diplomityö tehtiin Tampereen teknillisessä yliopistossa suoritetun diplomivaiheen opintojen opinnäytetyönä liittyen pääaineen syventäviin opintoihin kuuluvaan ainekokonaisuuteen tietoliikenneverkot ja protokollat.

Haluan kiittää SSP Yhtiöt Oy:tä mahdollisuudesta tehdä diplomityö heille ja molempia SSP Yhtiöt Oy:n ohjaajia Ville Isotaloa ja Antti Hurmetta työn ohjaamisesta ja mahdollisuudesta tutustua heidän yrityksensä pilvipalveluratkaisuihin. Ohjaus ja toiminnallisuuden näkeminen olivat merkittävässä osassa diplomityötä tehdessä ja ne auttoivat ymmärtämään pilvipalveluiden kokonaisuutta paremmin. Lisäksi haluan kiittää professori Jarmo Harjua hyvästä työn sisältöön ja jäsentelyyn liittyvästä ohjauksesta.

Koska tämä on viimeinen osasuoritus liittyen opintoihini Tampereen teknillisessä yliopistossa, haluan kiittää myös perhettäni siitä, että he jaksoivat olla tukenani koko opiskelujeni ajan.

SISÄLLYS

TERMIT JA NIIDEN MÄÄRITELMÄT

3DES	datan salaukseen käytetty algoritmi (Triple-DES).
ACL	pääsynhallintaan käytetty, tiettyyn objektiin sidottu lista luvista (Access Control List).
AES	datan salaukseen soveltuva spesifikaatio (Advanced Encryption Standard).
API	määrittelyrajapinta ohjelmien välistä kanssakäyntiä varten (Application Programming Interface).
DHCP	protokolla, joka jakaa automaattisesti uuden IP-osoitteen uudelle lähiverkkoon kytketylle laitteelle (Dynamic Host Configuration Protocol).
DNS	Internetin nimipalvelujärjestelmä, joka muuntaa verkkotunnuksia IP-osoitteiksi (Domain Name System).
ERSPAN	reititettävä versio RSPANista (Encapsulated Remote Switch Port Analyzer).
ESXi	VMwaren käyttämä nimitys omasta isäntäpalvelimestaan.
FT	VMwaren pilviympäristön lisäominaisuus, jonka tavoitteena on varmistaa fyysisten resurssien saatavuus virtuaalisten tietokoneiden palveluille ja sovelluksille ilman käyttökatkoa (Fault Tolerance).
GRE	Ciscon kehittämä IP-tunnelointiprotokolla (Generic Routing Encapsulation).
HA	VMwaren pilviympäristön lisäominaisuus, jonka tarkoitus on taata virtuaalisten palvelimien tarjoamien palveluiden ja sovellusten saatavuus vikatilanteissa (High Availability).
Hyper-V	Microsoftin käyttämä nimitys omasta isäntäpalvelimestaan.
IaaS	pilvipalvelumalli, jossa palveluntarjoaja tarjoaa koko infrastruktuurin palveluna (Infrastructure as a Service).

IPFIX	nimitys NetFlow-protokollan versiosta 10 ja sen avulla voidaan tarkkailla verkon liikennettä (IP Flow Information Export).
IPSec	IP-protokollan autentikointiin ja salaukseen tarkoitettu protokolla (Internet Protocol Security).
iSCSI	IP-protokollaan perustuva standardi levytilajärjestelmien kytkemisestä verkkoon (Internet Small Computer System Interface).
KVM	Linux kerneliin tehty virtualisointijärjestelmä, joka perustuu avoimeen lähdekoodiin (Kernel-based Virtual Machine).
LACP	Ethernet-protokolla, jonka avulla voidaan aggregoida fyysisesti erillisiä kytkimen portteja yhdeksi loogiseksi kanavaksi (Link Aggregation Control Protocol).
LBFO	Microsoftin käyttämä verkkoadaptereiden kuormantasaukseen, failoveriin ja ryhmitykseen tarkoitettu lisäominaisuus (Load Balancing and Failover).
LBT	VMwaren pilviympäristöissä toimiva verkkoliikenteen kuormantasaukseen liittyvä tekniikka (Load Based Teaming).
MAC-osoite	jokaisella verkkolaitteella oleva yksilöllinen laiteosoite (Media Access Control).
MTU	paketin tai kehyksen maksimikoko tavuissa (Maximum Transmission Unit).
NAS	tiedostotason verkkoon kytketty levytilajärjestelmä (Network-attached storage).
NAT	Internet-tekniikka, jonka avulla yhden julkisen IP-osoitteen alla voi olla useita yksityisiä IP-osoitteita (Network Address Translator).
NDIS	Microsoftin käyttämä verkkoadaptereiden ohjelmointirajapinta (Network Driver Interface Specification).

NIC	lyhenne fyysisestä verkkoadapterista (Network Interface Controller).
NVGRE	Microsoftin käyttämä verkon virtualisointi -teknologia, jonka tavoitteena on skaalautuvuuden parantaminen isoissa pilviympäristöissä (Network Virtualization using Generic Routing Encapsulation).
OID	tietyn objektin tunnus, jota Microsoft käyttää verkon hallintaan (Object Identifier).
OOB	tavallisesta verkkoliikenteestä erottuvaa siirtotietä hyödyntävä data, jota esimerkiksi Microsoft käyttää virtuaalisissa kytkimissä eteenpäinohjausta koskevan tiedon välitykseen (Out-of-band).
OSI-malli	tiedonsiirtoprotokollien yhdistelmää kuvaava viitemalli, joka erottaa protokollakerrokset toisistaan niiden toiminnallisuuden mukaan (Open Systems Interconnection Reference Model).
PaaS	pilvipalvelumalli, jossa palveluntarjoaja tarjoaa sovellusalustan palveluna (Platform as a Service).
PVLAN	yksityinen VLAN, jolla voidaan verkko segmentoida vielä tavallisen VLANin lisäksi (Private Virtual Local Area Network).
QoS	tarkoittaa tietoliikenteen luokittelua ja priorisointia (Quality of Service).
RRAS	Microsoftin palvelinrooli, jonka avulla voidaan toteuttaa reititykseen ja etähallintaan liittyviä toiminnallisuuksia (Routing and Remote Access Service).
RSPAN	etäyhteydellä toimiva, kytkimen porttikohtaisen verkkoliikenteen mahdollistama teknologia (Remote Switch Port Analyzer).
SaaS	pilvipalvelumalli, jossa palveluntarjoaja tarjoaa sovelluksen palveluna (Software as a Service).

SAN	arkkitehtuuri NAS-levytilajärjestelmien yhdistämiseksi niitä käyttäviin palvelimiin (Storage Area Network).
SDN	ohjelmallisesti toteutetun verkon konsepti (Software-defined Networking).
SNMP	TCP/IP-verkkojen hallinnassa käytettävä protokolla (Simple Network Management Protocol).
SPT	verkkoprotokolla, jonka tarkoituksena on poistaa siirtoyhteyskerroksen tasolla liikenteen kiertäminen edestakaisin (Spanning Tree Protocol).
SR-IOV	SR-IOV on standardi, joka mahdollistaa yhden PCI Express (PCIe) adapterin esittämisen loogisesti useana eri adapterina virtuaalisille tietokoneille (Single Root I/O Virtualization).
TCP	OSI-mallin kuljetuskerroksen tasolla tiedonsiirtoon käytetty protokolla (Transmission Control Protocol).
UDP	OSI-mallin kuljetuskerroksen tasolla tiedonsiirtoon käytetty protokolla (User Datagram Protocol).
VCNI	VMwaren luoma tekniikka yhdistää kaksi fyysisesti erillistä datakeskusta toisiinsa kapsuloinnin ja tunneloinnin avulla (vCloud Network Isolation).
VLAN	verkkotekniikka, jolla verkkoa voidaan segmentoida loogisesti (Virtual Local Area Network).
VNIC	lyhenne virtuaalisesta verkkoadapterista (Virtual Network Interface Controller).
VPN	kahden päätepisteen välille luotavan virtuaalisen tunnelin mahdollistama tekniikka (Virtual Private Network).
VTEP	VMwaren VXLANin tunneloinnin käyttämä päätepiste (Virtual Tunnel Endpoint).

VXLAN	VMwaren käyttämä verkon virtualisointiin liittyvä teknologia, jonka tavoitteena on yhdistää kaksi eri siirtoyhteyskerroksen verkkoa toisiinsa välissä olevan IP-verkon yli (Virtual Extensible Local Area Network).
WFP	Microsoftin kehittämä ohjelmointirajapintojen ja palveluiden joukko, jonka avulla voidaan luoda sovelluksia verkon liikenteen suodatukseen (Windows Filtering Platform).
WMI	Microsoftin hallintatyökalu esimerkiksi verkon virtualisointiin (Windows Management Instrumentation).

1 JOHDANTO

Pilvipalvelut ovat nykypäivänä merkittävä osa verkkopalveluita ja yleisesti verkkoarkkitehtuuria. Ne mahdollistavat esimerkiksi ohjelmistojen tilausperusteisen ja resurssien käyttöön perustuvan laskutuksen ja ovat siksi käytettävissä minkä kokoisissa yrityksissä tahansa. Pilvipalvelut ovat omana alanaan kasvattaneet arvoaan huomattavasti ja kasvun odotetaan jatkuvan edelleen. Pilvipalveluiden alaisuuteen kuuluu isona osana virtualisointi, sillä sen avulla mahdollistetaan esimerkiksi resurssien jakaminen julkisissa pilviympäristöissä. Tässä työssä käsitellään pilviympäristöjen toteutukseen liittyviä komponentteja ja niiden toiminnallisuutta.

Kuten pilvipalvelut, myös tietokoneiden resurssien virtualisointi on ollut käytössä jo pidemmän aikaa. Lähiverkon virtualisointi on kulkenut resurssien virtualisoinnin mukana ja sitä varten on kehitetty ratkaisuja eri valmistajien toimesta. Nämä lähiverkon virtualisoinnin ratkaisut ovat lähinnä ohjelmallisesti toimivia virtuaalisia kytkimiä. Miten jatkossa verkon virtualisointia voidaan laajentaa myös isäntälaitteiston ulkopuolelle laajentaen lähiverkko fyysisen verkon yli? Mitä ovat virtuaaliset kytkimet ja mitä eroa on eri valmistajien virtuaalisilla kytkimillä? Mitä tarkoittaa SDN-konsepti ja miten siihen ovat eri valmistajat reagoineet?

Tämä diplomityö pyrkii vastaamaan edellä mainittuihin kysymyksiin ja vertailemaan kahden suuren pilviympäristön valmistajan ratkaisuja. Työn luvussa 2 esitellään pilvipalveluiden perusteita ja luvussa 3 virtualisointiin liittyviä perusteita. Luvussa 4 esitellään kahden suuren valmistajan virtualisoidut kytkimet ja niiden toiminnallisuudet sekä esitellään lyhyesti vapaaseen lähdekoodiin perustuva virtuaalinen kytkin. Eri valmistajien tuotteita käsittelevissä luvuissa tarkastellaan lisäksi näiden valmistajien kehittämiä overlay-teknologia -ratkaisuja, joiden avulla lähiverkkoa voidaan laajentaa fyysisen verkon yli. Tarkasteluun kuuluvat näiden lisäksi myös muut lähiverkon virtualisointiin kehitetyt ratkaisut, kuten yhdyskäytävät, joiden avulla on mahdollista toteuttaa tärkeitä toiminnallisuuksia, jotka ovat verrattavissa perinteiseen verkkoarkkitehtuuriin.

Työn edetessä tehdään myös lähiverkon redundanttisuuden testaaminen toisen kaupallisen valmistajan pilviympäristössä hyödyntäen tämän valmistajan pilviympäristöön luomia lisäominaisuuksia, joilla saavutetaan korkea saatavuus ja vikatilanteesta toipuminen. Testaaminen haluttiin suorittaa, jotta voidaan todentaa kuinka hyvin valmistajan mainostamat toiminnallisuudet tositilanteessa toimivat. Edellä mainitut pilvipalvelun ja verkon redundanttisuuteen liittyvät asiat käsitellään luvussa 5, jossa esitellään aluksi lähiverkon redundanttisuuden testaamisessa käytettävät toiminnallisuudet ja tämän jälkeen käsitellään itse testausten suorittaminen ja sen tuottamat tulokset.

Luvussa 6 esiteltävä SDN-konsepti poikkeaa itsessään hieman pilviympäristöjen aiheesta, mutta on merkityksellinen verkon virtualisoinnin kannalta, sillä sen tavoite on saavuttaa keskitetty hallinta jo olemassa olevalle fyysiselle verkkoinfrastruktuurille ja mahdollistaa verkon toiminnan ohjaaminen ohjelmallisesti. SDN-konsepti on alun perin avoimeen lähdekoodiin perustuva, mutta myös kaupalliset yritykset ovat lähteneet kilpailemaan markkinoille omilla tuotteillaan. Näistä tuotteista esitellään VMware NSX ja Cisco ACI sekä pohditaan lisäksi niiden yhdenmukaisuutta SDN-konseptin kanssa.

Työ päättyy luvun 7 yhteenvetoon, jossa pohditaan tarkasteltujen ratkaisujen ja toimintojen sekä konseptien tarkoituksenmukaisuutta, mahdollisuuksia tulevaisuudessa ja niihin mahdollisesti liittyviä ongelmia niin käyttöönotossa kuin itse käytössä.

Työ suoritettiin SSP Yhtiöt Oy:n toimeksiannosta. Työ perustuu suurelta osin valmistajien dokumentaatioihin omista tuotteistaan sekä lähiverkon redundanttisuuden testauksessa käytännön kokeiluun.

2 PILVIPALVELU

Pilvipalvelulla tarkoitetaan palveluntarjoajan tilausperusteista palvelua, josta tilaaja saa itselleen laskentaresursseja toimintojen suorittamiseen ja levykapasiteettia tiedonsäilytykseen. Yksinkertaisemmin sanottuna yritykset voivat siirtää omat palvelunsa omista tiloistaan palveluntarjoajien konesaleihin tai luoda oman pilven, jossa yritys jakaa palveluita yrityksen sisäisesti. Hyvin pilvipalveluita kuvaava esimerkki on sähköpostipalvelu, jossa palvelun tilaaja saa sähköpostitilin käyttöoikeuden ja tietyn määrän levykapasiteettia sekä myös ohjelmiston, joka suoritetaan palveluntarjoajan palvelimella. Tässä esimerkissä palvelun tilaaja voi kirjautua mistä tahansa maantieteellisestä sijainnista palveluun Internet-selaimen avulla ilman, että tilaajan tarvitsee itse sijoittaa rahaa ohjelmiston hankintaan tai sen ylläpitämiseen. Internet-selaimen kautta toimivat sähköpostipalvelut ovat myös riippumattomia alustasta, eli esimerkiksi tietokoneesta tai älypuhelimesta, joilla niitä käytetään. Sähköpostipalvelussa sijaitsevat viestit, jotka veisivät muistikapasiteettia tilaajan omalta tietokoneelta, voidaan säilyttää palvelimella. Tämä esimerkki on kuitenkin vain yksi osa pilvipalveluita ja siitä käytetään nimitystä SaaS (Software as a Service). SaaS:n lisäksi on olemassa IaaS (Infrastructure as a Service) ja PaaS (Platform as a Service) -palvelumallit joista kerrotaan tarkemmin tämän luvun myöhemmissä kappaleissa. Yksi suurimmista pilvipalveluista on Facebook, joka voidaan muiden sosiaalisten verkostojen kanssa lukea pilvipalveluiksi. Facebook tarjoaa PaaS-palvelumallilla toimivan vaihtoehdon sosiaalisia verkostoja hyödyntäville sovelluksille. [1 ; 2, s. 39]

Pilvipalvelu voidaan myös ajatella niin, että fyysisesti kaukanakin oleva palvelu voidaan tuoda loogisesti tilaajan lähelle. Tämä tukee myös pilvipalvelun mieltämistä abstraktioksi, sillä esimerkiksi pilvipalvelun etäisyys ei näy tilaajalle sen erikoisemmin, se vain on olemassa oleva palvelu, johon tilaaja pääsee mistä tahansa.

Pilvipalveluiksi voidaan myös mieltää vertaisverkot (peer-to-peer), sillä niissä asiakkaat muodostavat yhdessä verkon, jonka kautta voidaan jakaa sisältöä, kuten musiikkia, videoita ja tietokoneohjelmia. Myös vertaisverkoissa pilvipalvelun abstraktio tulee vahvasti esille, sillä vertaisverkko muodostuu maantieteellisesti hajautetuista yksittäisten tietokoneiden muodostamasta verkosta. [2]

2.1 Pilvipalvelun edut

Pilvipalvelut ovat suhteellisen uusi asia, varsinkin Suomessa. Niiden levinneisyys saattaa johtua erilaisista asioista, mutta yksi merkittävä asia on, että niiden etuja ei ymmärretä täysin. Toki on olemassa yrityksiä, joilla ei ole tarvetta siirtyä pilvipalveluiden käyttöön, ainakaan täysin, mutta kaikkien tulisi silti tiedostaa mahdolliset pilvipalveluis-

ta saatavat hyödyt verrattuna perinteiseen IT-malliin. Seuraavaksi esitellyt pilvipalveluiden edut eivät ole itsestään pilvipalveluun kuuluvia, vaan ne muodostuvat useista eri pilvipalvelusovelluksista.

Pilvipalvelut ovat joustavia. Pilvipalveluiden avulla oma liiketoiminta ja erityisesti liiketoimintaa tukevat sovellukset voidaan siirtää pilveen. Tämä tarkoittaa sitä, että yrityksen ei tarvitse huolehtia laitteistosta, mikä suorittaa näitä ohjelmistoja. Tämä tarkoittaa samalla sitä, että yrityksen ei myöskään tarvitse huolehtia riittävätkö laitteiston resurssit palvelemaan kaikkia sen käyttäjiä. Pilvipalvelut ovat siis hyvin joustavia ja skaalautuvia, mikäli yrityksellä tulee tarve laajentaa toimintaansa.

Kun yrityksen tietojärjestelmissä tapahtuu vikatilanne, pilvipalveluntarjoajat pitävät huolen siitä toipumisesta. Mikäli käytössä on perinteinen IT-malli, saattaa vian aiheuttaja olla esimerkiksi fyysinen laitteisto, jolloin vian korjaus maksaa paljon ja kestää kauan. Pilvipalveluntarjoajat pystyvät taas tarjoamaan nopean viankorjauksen ja jopa palvelun, jonka avulla käyttökatkoja ei tule.

Automaattiset ohjelmistopäivitykset helpottavat toimintaa, sillä manuaalisesti tehtyihin päivityksiin kulutetaan yrityksissä aikaa hyvin paljon. Pilvipalveluissa palveluntarjoaja huolehtii laitteiston päivittämisestä ja tietoturvapäivityksistä. Myös ohjelmistojen päivitykset voidaan suorittaa keskitetysti, jolloin jokaisen erillisen työaseman päivitys ei ole tarpeellista.

Pilvipalvelut ovat pääomavapaita. Useimmat pilvipalveluntarjoajat myyvät palveluitaan kulutukseen perustuvaan hinnoitteluun perustuen. Tämä tarkoittaa, että yrityksen ei itse tarvitse sijoittaa esimerkiksi palvelinlaitteisiin pääomaa ja huolehtia niiden vanhenemisesta. Myös palvelun käytön aloittaminen on edullista, koska laiteinvestointeja ei tarvitse tehdä.

Parantunut yhteistyö työntekjöiden välillä on mahdollista pilvipalveluiden avulla. Pilvipalveluiden avulla työntekijät voivat jakaa dokumentteja keskenään missä he ikinä ovatkaan. Kriittiset viestit ja päivitykset saavuttavat kaikki työntekijät samanaikaisesti ja he pystyvät kommunikoimaan keskenään entistä tehokkaammin. Pilvipalvelut poistavat usein rajoitteen myös siitä, käyttääkö työntekijä omaa laitettaan vai yrityksen antamaa laitetta omalla työpisteellään.

Pilvipalveluiden avulla on mahdollista tehdä töitä mistä tahansa kunhan työntekijällä on pääsy Internetiin. Etätyömahdollisuus saavutetaan pilvessä sijaitsevien ohjelmistojen ja palveluiden avulla ja se mahdollistaa tehokkaan työskentelyn myös työmatkoilla kuin myös tarvittaessa kotona.

Dokumentin hallinta helpottuu pilvipalveluiden avulla, sillä niitä hyödyntämällä työntekijät tai muut useat käyttäjät voivat esimerkiksi muokata yhtä dokumenttia samanaikaisesti eri puolilta maapalloa. Perinteisessä IT-mallissa joudutaan lähettämään sähköpostin välityksellä dokumentteja edestakaisin kun kaksi työntekijää käsittelee niitä vuorotellen ja lähettää päivitetyn version toiselle. Pilvipalvelussa dokumentit sijaitsevat yhdessä paikassa ja niihin tehdyt muutokset tulevat voimaan välittömästi, jolloin toinen työntekijä saa välittömästi käyttöönsä päivitetyn version dokumentista.

Pilvipalvelut luovat tiettyä turvallisuutta. Esimerkiksi kadonneet tai hajoavat tietokoneet eivät ole pilvipalveluiden kanssa ongelma, sillä ohjelmistot ja tiedot ovat pilvessä. Näin ollen varastettu kannettava työtietokone ei itsessään sisällä liiketoiminnalle kriittisiä tietoja, vaan niiden saamiseksi tulee saada pääsy pilveen

Pilvipalveluilla saavutetaan kilpailukykyä. Pilvipalveluiden avulla esimerkiksi toipuminen vikatilanteista IT-järjestelmissä on huomattavasti nopeampaa kuin perinteisissä järjestelmissä. Tämän lisäksi uusien sovellusten käyttöönotto on huomattavasti nopeampaa pilvijärjestelmän avulla, sillä esimerkiksi uuden virtualisoidun palvelimen käyttöönotto onnistuu ilman laitteiston hankintaa ja sen erillistä konfigurointia.

Pilvipalvelut ovat lisäksi ympäristöystävällisiä. Virtualisoinnin ansiosta ne vievät vähän tilaa ja kuluttavat energiaa vähemmän kuin perinteiset palvelinratkaisut. Pilvipalveluiden käytön on laskettu vähentävän energiankulutusta jopa 30% verrattuna perinteiseen IT-järjestelmään. [3]

2.2 Pilven jakelutyypit

Pilvi voidaan jakaa eri jakelutyyppeihin niiden toimintamallin ja osittain myös topologian mukaan, vaikka pilvi usein abstraktina käsitteenä nähdäänkin.

Private cloud eli yksityinen pilvi on pilvi, joka on näkyvissä ainoastaan halutuille tilaajille. Esimerkiksi yrityksen sisäiset tietoverkkotoiminnot, joilla voidaan toteuttaa erilaisia yrityksen liiketoimintaa tukevia ohjelmistoja (CRM, tiedostojen jakaminen, ym.), sijaitsevat yksityisessä pilvessä, joten yrityksen ulkopuolelta pilveen ja sen sisältämiin palveluihin ei pääse. Yksityinen pilvi onkin erinomainen tapa jakaa yrityksen sisäisessä käytössä olevia palveluita koska palvelut saadaan sijoitettua yhteiseen paikkaan ja näin ollen jokainen yrityksen päätelaite ei tarvitse erillistä ohjelmistoa, mikä taas on yritykselle kustannustehokasta. Yksityinen pilvi voi toki sisältää ainoastaan tietokannan, jolloin tietokoneissa olevat ohjelmistot hakevat pilvestä tiedot esimerkiksi asiakkaista. Yksityistä pilveä hyödyntävät esimerkiksi ohjelmistotalot, joissa sovelluskehittäjille voidaan antaa oma yksityinen tila pilvestä, jonne he voivat luoda palvelimia sovellusten testaamista varten.

Public cloud eli julkinen pilvi tarkoittaa sitä, että se on kaikkien saatavilla, eli pilvessä toteutettu palvelu on käytettävissä julkisen verkon kautta. Näin ollen julkisessa pilvessä oleva kapasiteetti ovat kaikkien sen asiakkaiden käytössä. Vaikka kapasiteetti onkin kaikkien käyttäjien käytössä, voidaan silti tietyt palvelut julkisessa pilvessä pitää suljettuina niin, että ne ovat käytössä vain tietyistä paikoista. Teknisesti julkisen ja yksityisen pilven välillä ei välttämättä ole suuria eroja, mutta erot syntyvät tietoturvan ja niiden palveluiden kautta, joita julkiselle puolelle tarjotaan eli palveluntarjoajat voivat antaa tietyt palvelut julkiseen käyttöön, mutta rajoittaa tietyt palvelun vain yksityisen pilven käyttäjille.

Community cloud eli yhteisöpilvi tarkoittaa kahden tai useamman organisaation jakamaa pilvipalvelua. Se on siis tavallaan useamman toimipisteen yksityinen pilvi, johon ulkopuoliset eivät pääse. Nämä organisaatiot tai vaihtoehtoisesti toimipisteet voi-

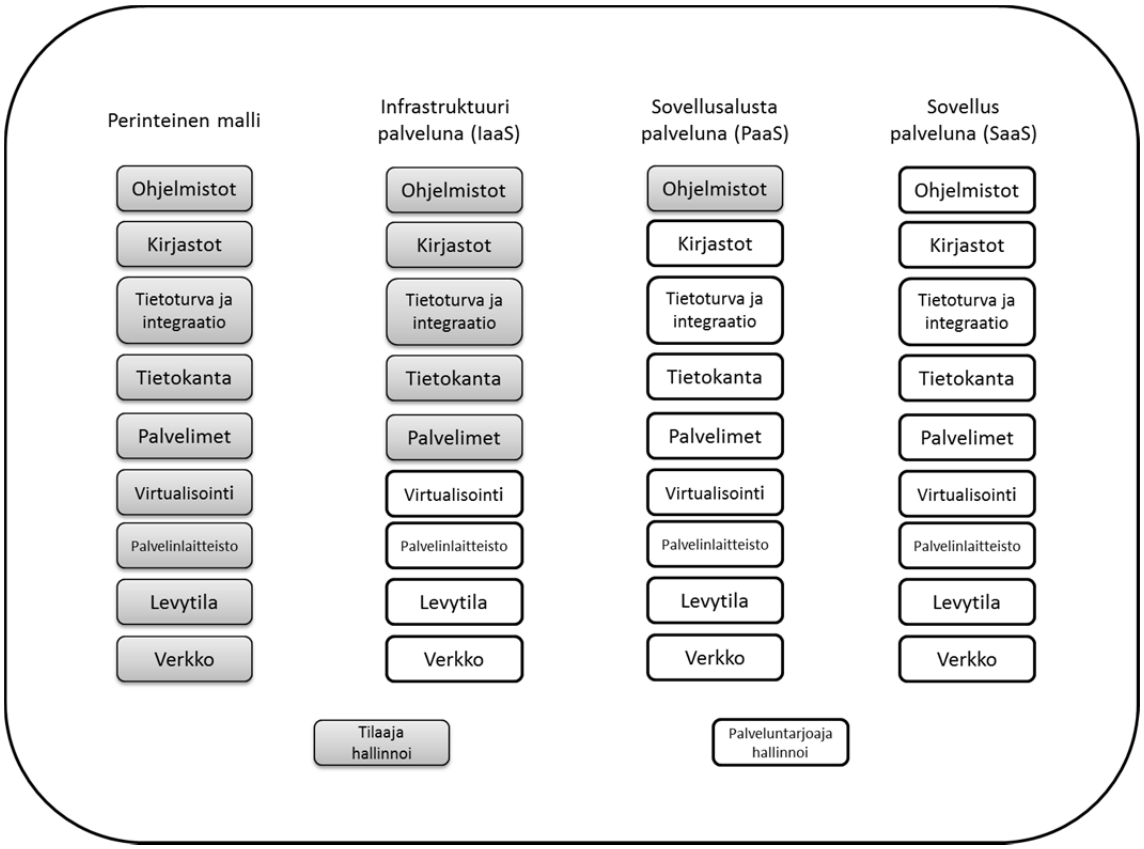
vat siis sijaita maantieteellisesti eri sijainneissa, mutta niille molemmille pilvessä olevat palvelut ja pilven toimintaperiaatteet ovat yhteiset.

Hybrid cloud eli hybridipilvi on yhdistelmä edellä mainituista pilvityypeistä tai osasta niitä. Hybridipilvi voi siis koostua yksityisestä pilvestä, julkisesta pilvestä ja yhteisöpilvestä tai niiden erilaisista kombinaatioista. Oleellista on, että hybridipilvessä osa palveluista voidaan pitää yksityisen pilven tavoin vain tiettyjen tilaajien saatavilla ja osa voidaan taas pitää julkisina palveluina. Näin ollen ei voida tehdä selkeää eroa, onko pilvi yksityinen vai julkinen. Hybridipilvi voidaan toteuttaa monella eri tavalla ja palveluntarjoaja määrääkin mitkä palvelut ovat kenenkin saatavilla ja mistä sijainneista. Hybridipilvi voidaan määrittää myös niin, että osa pystyy käyttämään tiettyjä palveluita SaaS-mallin mukaan, mutta osa pystyy hyödyntämään pilveä laajemmin. Hybridipilven avulla voidaan myös toteuttaa vikasietoisuutta, sillä vaikka julkinen Internet-yhteys katkeaisi, voidaan silti käyttää yksityisen pilven tarjoamia palveluita normaalisti. Esimerkkinä hybridipilven muista hyödyistä on cloud bursting, jonka avulla laskentaresursseja voidaan tarpeen vaatiessa ottaa toisesta pilvestä, esimerkiksi silloin kun tiettyjä ohjelmistoja tai palveluita käytetään niin paljon, että yksittäisen pilven kokonaislaskentateho ei riitä prosessoimaan kaikkea. [4]

Distributed cloud eli jaettu pilvi ei tarkalleen ottaen ole pilven jakelutyyppi, vaan pilvilaskennan jakelumalli, jossa pilvi on usean eri paikassa sijaitsevan tietokoneen yhdistetty kokonaisuus. Jaetussa pilvessä voidaan yhdistää eri tietokoneiden ylimääräiset laskentaresurssit yhteiseksi ja näin ollen voidaan hyödyntää laskentatehoa esimerkiksi lääketieteellisiin tutkimuksiin. Jaetussa pilvessä tietokoneet sijaitsevat eri paikoissa, mutta ovat silti loogisesti yhteydessä samaan verkkoon. Esimerkiksi Folding@home ja BOINC (Berkeley Open Infrastructure for Network Computing) ovat jaetun pilven resursseja hyödyntäviä projekteja. Esimerkiksi Folding@home projektissa käytettiin vapaaehtoisten Playstation 3 -pelikonsolien käyttäjien jakamia resursseja lääketieteellisien tutkimusten apuna. Tämä toteutettiin yksinkertaisesti niin, että käyttäjä käynnisti konsoliin valmiiksi asennetun ohjelmiston ja jakoi näin oman konsolinsa laskentatehon muuhun käyttöön verkon kautta.

2.3 Pilvipalvelumallit

Pilvipalvelut jaetaan yleisesti kolmeen tasoon, IaaS-, PaaS- ja SaaS-palvelumalleihin. Niiden erot ovat teknisiä, mutta ne ovat myös liiketoiminnan kannalta poikkeavia. Pilvipalvelumallien avulla tilaaja saa selkeän kuvan pilvipalveluiden eri tasoista ja voi tilata juuri tarvitsemansa palvelun. Tärkeintä tietenkin tilaajan kannalta on, että tilaaja saa mahdollisimman hyvin liiketoimintaprosessejaan tukevan palvelun, eikä se millä tekniikalla palvelu on toteutettu. Alla olevassa kuvassa (Kuva 1) on pilvipalvelumallien tasot verrattuna perinteiseen IT-malliin esitettynä hallinnoinnin näkökulmasta.



Kuva 1: Perinteinen IT-malli ja pilvipalvelumallit esitettynä eri tasojen avulla, joita hallinnoi joko tilaaja tai palveluntarjoaja. [1]

2.3.1 Infrastruktuuri palveluna (IaaS)

Laajimmassa pilvipalveluiden palvelumallissa IaaS:ssä palveluntarjoaja tarjoaa koko infrastruktuurin palveluna. Tämä tarkoittaa sitä, että tilaaja saa palveluntarjoajalta käyttöönsä fyysiset tai virtuaaliset tietokoneet, jotka ovat pilvipalvelun ydin. Pilvipalveluissa käytetään useimmiten virtuaalisia tietokoneita. Itse isäntä on fyysinen laitteisto, mutta näihin fyysisiin isäntiin voidaan asentaa useita virtuaalisia tietokoneita, guesteja eli vieraita. Virtualisoinnista lisää luvussa 3. Kun kyseessä on IaaS -palveluluokka, niin perusoletuksena tilaaja saa siis laitteiston resurssit käyttöönsä ja voi resurssien avulla toteuttaa pilvipalvelun omien tarpeidensa mukaan. Perinteisestä ulkoistamisesta IaaS-palvelumalli eroaa joustavuudessa, resurssien yhteiskäytössä, itsepalvelussa, automaatiossa ja käyttöön perustuvassa laskutuksessa [2]. IaaS -palvelumallissa voidaan tarjota lisäksi vielä erilaisia lisäpalveluita kuten palomuureja, virtuaalisia lähiverkkoja, IP-osoitteita tai kuorman jakamista. Viimeistään näiden lisäpalveluiden avulla IaaS:stä muodostuu siis muokattava alusta pilvipalvelulle ja näin ollen pohja PaaS:lle eli palvelualustalle. IaaS-palvelumallissa tilaajat asentavat pilveen haluamansa käyttöjärjestelmän ja ohjelmistot, kuten mahdolliset palvelinohjelmistot, käyttäen valmiiksi asennettuja käyttöjärjestelmiä mallipohjien avulla tai perinteisesti CD-ROM-levykuvan (ISO-tiedosto) kanssa. Tilaajan on hyvin usein mahdollista saada IaaS-palvelumallissa juuri

niin paljon resursseja palveluiden käyttöön, kuin on tarpeen ja kun laskutusperusteet ovat usein resurssien käytön mukaan, on tämä myös edullista tilaajalle. Tilaajalle pilvipalvelun edulliseksi tekee myös oman konesalin tarpeettomuus ja paljon resursseja vaativien palveluohjelmistojen käyttäminen palveluntarjoajan laitteiston avulla.

2.3.2 Sovellusalusta palveluna (PaaS)

PaaS-palvelumallissa tilaaja saa palveluntarjoajalta alustan ja tietyt ohjelmistot sekä valmiudet rakentaa pilvipalvelunsa omalla sisällöllään. Suurin ero IaaS-palvelumalliin tuleekin siitä, että PaaS-palvelumalli sisältää valmiiksi ohjelmistot ja kirjastot, joiden päälle tilaaja voi pilvipalvelun muodostaa. PaaS-palvelumallit eroavat palveluntarjoajien mukaan ja yhdenlaista PaaS-mallia ei varsinaisesti olekaan. PaaS-palvelussa tilaaja saa itselleen siis fyysisen laitteiston käyttöoikeuden resursseineen sekä alustan, kuten ESXi Host, Microsoft Hypervisor tai KVM ja voi näiden ohjelmistojen ja levykuvien avulla luoda minkälaisen PaaS-ympäristön haluaa. PaaS-palvelu voi sisältää myös lisäpalveluita, kuten ohjelmistojen suunnittelua, luontia, kehitystä sekä testausta, tietoturvaa, levykapasiteettia, skaalautuvuutta ja valmiita ohjelmistoja. PaaS-palvelumallia kannattaakin ajatella astetta valmiimpana kokonaisuutena kuin IaaS-palvelumallia.

Valmiit PaaS-tarjoomat voidaan jakaa kolmeen osa-alueeseen: PaaS sidottuna SaaS -ympäristöön, PaaS sidottuna IaaS -ympäristöön ja avoimen alustan PaaS. Näillä PaaS-tarjoomilla tarkoitetaan esimerkiksi Salesforce.comin, Force.comin, Googlen AppEnginen Microsoft Azure Platformin tarjoamia sovellusalustoja, joiden päälle sovelluksia voidaan kehittää ja joilla niitä voidaan testata, ylläpitää ja kehittää. PaaS sidottuna SaaS-ympäristöön tarkoittaa, että SaaS-palvelun valmistajat mahdollistavat kolmannen osapuolen luoda ohjelmistoja oman PaaS-ympäristönsä päälle. Tämä tarkoittaa siis sitä, että ohjelmistot, joita tilaaja voi PaaS-ympäristöönsä asentaa ja käyttää, voidaan luoda kolmannen osapuolen toimesta valmiiksi. Tämä kuitenkin rajoittaa PaaS-palvelun käyttöä, sillä tämänkaltaiseen PaaS-palveluun asennettavat ohjelmistot vaativat juuri tietyn PaaS-ympäristön. PaaS sidottuna IaaS-ympäristöön taas tarkoittaa sitä, että IaaS-palvelussa tilaaja saa fyysisen laitteiston lisäksi työkalut luoda juuri tähän tiettyyn fyysiseen laitteistoon soveltuvia ohjelmistoja. Tämä on hyvä PaaS-palvelumalli siinä tapauksessa, jos tilaajalle on edullista käyttää vain yhden valmistajan toimittamia fyysisiä laitteistoja IaaS-palvelussa. Ongelmia saattaa kuitenkin tulla, mikäli halutaan laajentaa pilveä ja laitteiston tulee olla sama, jotta siihen asennetut ohjelmistot toimivat keskenään. Avoimen alustan PaaS-malli taas on nimensä mukaan avoin, eikä sitä ole sidottu mihinkään tiettyyn laitevalmistajaan tai SaaS-ympäristöön. Avoimen alustan PaaS-malli voidaan ajatella esimerkiksi virtualisoiduksi palvelimeksi, joka toimii sovellusalustana, eikä näin ollen millään tavalla laitevalmistajasta riippuvainen. Tämä malli tarjoaa parhaiten joustavuutta, sillä PaaS-valmistajat antavat ohjelmistokehittäjien tuoda omat ohjelmistonsa pilveen, mutta se saattaa näin muodostua myös kalleimmaksi ja monimutkaisimmaksi ratkaisuksi. Tämä malli sopii parhaiten hybridipilvi-jakelumalliin, sillä se mahdollistaa ohjelmistojen julkaisemisen sekä yksityisissä että julkisissa pilvissä edelleen riippumatta valmistajista tai SaaS-palveluista. Avoimen alustan mallin kanssa tulee

kuitenkin olla tarkkana, sillä tietyt ohjelmistot vaativat tiettyjä ominaisuuksia, kuten .NET ohjelmistokomponenttikirjaston, jotta ne toimivat halutulla tavalla. [5]

2.3.3 Sovellukset palveluna (SaaS)

SaaS-palvelumalli on ylimmän tason pilvipalvelumalli, jossa tilaaja saa valmiin alustan, johon kuuluvat IaaS- ja PaaS -palvelumallien sisältämät palvelut ja voi näin ollen keskittyä pilvessä vain ohjelmistojen käyttämiseen ja mahdollisesti ylläpitämiseen. Useimmissa tapauksissa ohjelmiston ylläpito kuitenkin kuuluu palveluntarjoajalle ja se on yksi syistä miksi tilaaja valitsee pilvipalvelun tavallisen ohjelmiston sijaan. SaaS-palvelumallissa tilaaja saa siis valmiin ohjelmiston käytettäväkseen eikä maksa näin lisenssipohjaisesti ohjelmistosta vaan tilaa sen palveluna. Hyvin usein SaaS-palvelut ovat Internet-selaimella toimivia ohjelmistoja. Internet-selaimella tilaaja pääsee siis pilvessä sijaitsevaan ohjelmistoon ja käyttää ohjelmistoa sen kautta. Lisäksi on tärkeää ymmärtää, että ohjelmisto jota käytetään, on yhteinen kaikille sen käyttäjille eikä asiakaskohtaisia tietokoneelle asennettavia ohjelmistoja ole. SaaS-palvelumallin ohjelmistot voivat olla esimerkiksi CRM-ohjelmistoja (asiakkuudenhallinta), ERP-ohjelmistoja (toiminnanohjausjärjestelmä), kirjanpito-ohjelmistot tai HRM-ohjelmistoja (henkilöstönhallinta). SaaS-palvelumalli on yleisin ja suosituin palvelumalli, sillä sen avulla organisaatiot saavat ulkoistettua ohjelmistojen vaatiman laitteiston ylläpidon ja hankintakuluja ei tule. SaaS-palvelumallissa laskutus perustuu usein ohjelmistojen laajuuteen. Perinteiseen ohjelmistoon verrattuna SaaS-palvelut ovat myös nopeasti käyttöönotettavia ja tilaajan ei tarvitse huolehtia ohjelmistojen ostamisesta, asentamisesta tai päivittämisestä.

SaaS-palvelumalli voidaan luokitella kolmeen kategoriaan [6], pakatut ohjelmistot (Packaged software), yhteisohjelmistot (Collaborative software) ja hallintatyökalut (Enabling and management tools). Pakatuilla ohjelmistoilla tarkoitetaan valmiita yritystoimintaa tukevia ohjelmistoja kuten asiakkuudenhallinta-, toimitusketjun hallinta-, taloudenhallinta- ja henkilöstönhallintaohjelmistot. Nämä ohjelmistot ovat monelle yritykselle hyvin tärkeitä liiketoiminnan kannalta, mutta ne eivät ole SaaS-palvelumallin käytetyin kategoria. Yhteisohjelmistot tulevat tarpeesta jakaa tietoja yhteisesti tiettyjen tahojen kanssa riippumatta fyysisestä sijainnista, joten yhteisohjelmistoihin kuuluvat esimerkiksi web-konferenssi-, dokumenttien yhteiskäyttö-, projektien suunnittelu-, pikaviestintä- ja jopa sähköpostiohjelmistot. Yhteisohjelmistot voidaan luokitella suurimmaksi ja suosituimmaksi kategoriaksi SaaS-palvelumallissa. Yhteisohjelmistoihin voidaan luokitella myös tiedon ja tiedostojen jakamiseen, tehtävälistojen laadintaan, ajankäytön hallintaan ja reaaliaikaiseen viestintään kuuluvat pilvipalvelut. Tämänkaltaista pilvipalvelua tarjoaa esimerkiksi 37 signals niminen yritys, jonka Basecamp-ohjelmisto on projektinhallinta- ja viestintätyöväline. Yritys on merkinnyt Basecamp-ohjelmistonsa asiakasreferensseiksi esimerkiksi WWF:n, Warner Bros:n, Kellogsin, National Geographicin ja Adidaksen. Viimeiseen kategoriaan eli hallintatyökaluihin lukeutuvat esimerkiksi testaus-, valvonta- ja mittausohjelmistot. Hallintatyökalut ovat

tärkeä, vaikkakin näkymätön osa SaaS-palvelumallia, sillä sen avulla ohjelmistokehittäjät voivat testata sovelluksiaan ja kehittää tilaajan saamaa palvelua eteenpäin.

Hyvä esimerkki muistakin SaaS-palvelumallin mahdollisuuksista on digitaalisen sisällön tuottaminen. Autodeskin Project Twitch on juuri tällainen. Autodesk on yhdysvaltalainen yritys, joka on tunnettu erityisesti AutoCAD suunnitteluohjelmistostaan ja Project Twitch on Autodeskin kehittämä pilvipalveluun perustuva versio yrityksen eri sovelluksista. Käytännössä tilaaja voi siis käyttää Autodeskin AutoCAD-, Revit-, Inventor- ja Maya-sovelluksia Internet-selaimella. Tässä tapauksessa on otettava huomioon, että Project Twitch on tehty pääsääntöisesti ohjelmistojen kokeilua varten, mutta tämä kertoo myös siitä, miten monimuotoisia ovat pilvipalveluiden mahdollisuudet.

3 VIRTUALISOINTI PILVIPALVELUISSA

Pilvipalvelut voidaan toteuttaa niin fyysisinä kuin myös virtualisoituina palveluina. Pilvipalvelussa on toki aina fyysinen osa, joka sisältää laskentatehon ja muut resurssit, mutta virtualisointi on tapa, jolla fyysisestä osasta saadaan huomattavasti joustavampi ja skaalautuvampi palvelu. Immo Salo määrittelee virtualisoinnin kirjassaan Cloud Computing seuraavasti: ”Virtualisointi tarkoittaa tekniikkaa, jolla jonkin fyysisen resurssin tekniset piirteet piilotetaan muilta järjestelmiltä, sovelluksilta ja loppukäyttäjiltä, jotka käyttävät näitä resursseja. Tällöin yksi fyysinen resurssi, kuten palvelin, käyttöjärjestelmä, sovellus, tallennusväline tai verkko, voi toimia monena loogisena resurssina, tai useat fyysiset resurssit, kuten tallennuslaitteet, palvelimet tai verkkoliitännät, näkyvät yhtenä loogisena resurssina.” Voidaan siis sanoa, että virtualisoinnin tarkoitus on poistaa laitteisto- ja sovelluskohtaiset rajoitteet rajapintojen välistä ja parantaa skaalautuvuutta, sekä hyödyntää fyysiset resurssit mahdollisimman tehokkaasti. [2, s. 47]

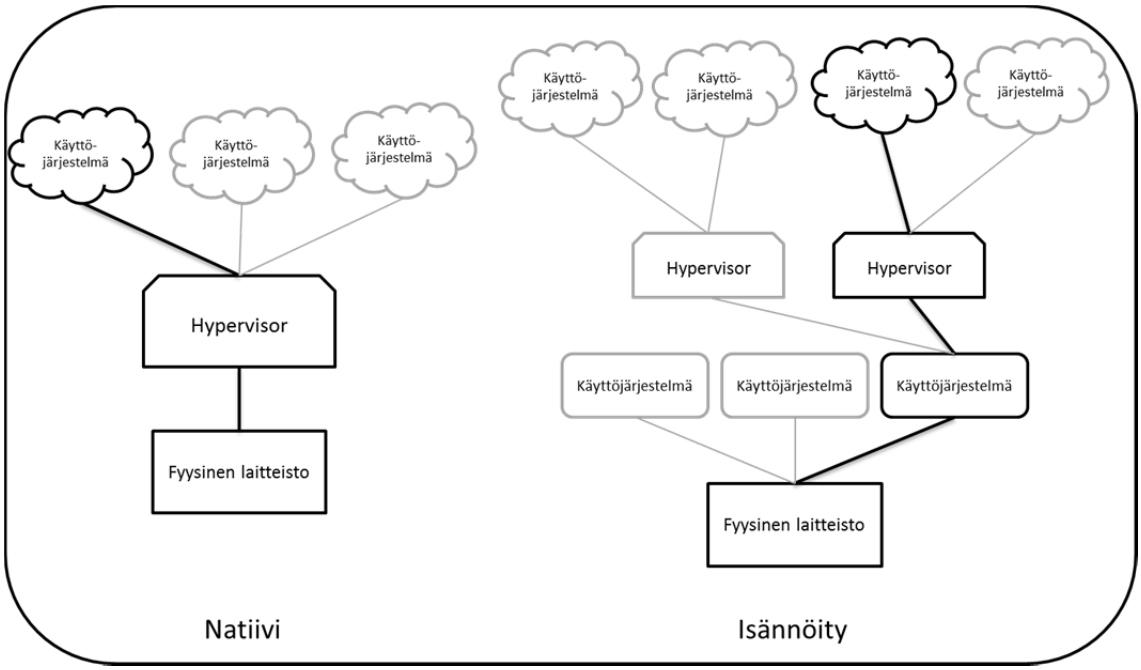
Virtualisointi voidaan tehdä monella eri tasolla. Kuten luvun aloituskappaleessa mainittiin, virtualisoida voidaan palvelin eli itse laitteisto, työpöytä, levytila ja verkko. Nämä voidaan luokitella pääkategorioiksi kun puhutaan virtualisoinnista, mutta ne ovat kuitenkin vain osa mahdollisista virtualisoitavista kohteista ja ne sisältyvät osittain toisiinsa. Muita virtualisoinnin kohteita ovat lisäksi esimerkiksi sovellusten virtualisointi, palvelun virtualisointi ja muistin virtualisointi. Virtualisoinnilla on sen antamien etujen lisäksi myös haittapuoli, sillä sen seurauksena arkkitehtuuriin syntyy uusi kerros, joka on sekä kustannus kaupallisissa ratkaisuissa että monimutkaisuutta lisäävä tekijä, joka taas saattaa aiheuttaa tietoturvariskin. Seuraavissa luvuissa esitellään tarkemmin ne virtualisoinnin tasot, jotka ovat oleellisia pilvipalveluissa käytetyn virtualisoinnin ymmärtämiseksi.

3.1 Palvelinvirtualisointi

Palvelimella tarkoitetaan perinteisessä IT-mallissa palvelinohjelmistoa ja fyysistä palvelinlaitteistoa, jonka tarkoitus on tarjota asiakkaalleen jokin palvelu joko omassa verkossa tai Internetin välityksellä. Perinteisen palvelinmallin heikkoja kohtia ovat esimerkiksi laitteen hankintakulut sekä resurssien vajaakäyttö. Palvelinohjelmisto käyttää vain tietyn osan palvelinlaitteiston resursseista ja näin ollen osa resursseista menee hukkaan. Vaikka palvelinlaitteisto olisi määritetty mahdollisimman sopivaksi juuri tietylle palvelinohjelmistolle, tulee ylläpitäjän ottaa huomioon mahdolliset piikit käyttöasteessa, eli tilanteet, jolloin palvelinta käyttää normaalia käyttöastetta suurempi määrä asiakkaita. Tällaisessa tilanteessa resurssit saattavat joko loppua kesken tai niitä saattaa jäädä yli. Tietysti ylläpitäjät pyrkivät aina tilanteeseen, jolloin resurssit riittävät kaikkien asiak-

kaiden palvelemiseksi, mutta tilanteet saattavat olla vaikeita arvioida ennalta. Palvelimen virtualisoinnissa palvelinohjelmisto käyttää resursseja juuri niin paljon kuin se tarvitsee ja näin ollen resurssien käyttöaste pysyy toivotussa. Palvelimen ylläpitäjän ei myöskään tarvitse huolehtia laitteiden hankinnasta, ellei ole itse toteuttamassa sitä, vaan voi keskittyä itse palvelinohjelmiston ylläpitämiseen. Virtualisoinnissa fyysisenä laitteistona käytetään tehokkaita palvelinkoneita, joihin on mahdollista asentaa useita eri palvelinohjelmistoja. Palvelinohjelmistot käyttävät fyysisen laitteiston resursseja juuri niin paljon kuin ne niitä tarvitsevat ja ylijäävä osa on muiden palvelinohjelmistojen käytössä. Toinen suuri etu palvelimen virtualisoinnissa on nopea palvelinohjelmistojen provisiointi. Kun perinteisessä palvelinmallissa halutaan ottaa uusi palvelinohjelmisto käyttöön tai esimerkiksi luoda kopio vanhasta palvelinohjelmistosta, pitää ylläpitäjän hankkia uusi fyysinen laitteisto ja konfiguroida kaikki uudelleen, jolloin aikaa uuden palvelinohjelmiston käyttöön kuluu paljon enemmän. Palvelimen virtualisoinnissa voidaan uusi palvelinohjelmisto asentaa suoraan nykyiselle fyysiselle palvelinlaitteistolle, jolloin se toimii vanhan palvelinohjelmiston kanssa fyysisesti rinnakkaisena, mutta loogisesti erillisenä palvelimena. Myös vanhan palvelinohjelmiston kopiointi uudeksi rinnakkaiseksi palvelinohjelmistoksi onnistuu nopeasti, sillä vanhasta palvelinohjelmistosta voidaan ottaa suoraan levykuva, jolloin siihen tehdyt konfiguraatiotkin siirtyvät mukana. Edut laitehankintojen kuluihin syntyvät erityisesti silloin, kun asiakas tilaa pilvipalvelun palveluntarjoajalta, jolloin fyysinen laitteisto sijaitsee palveluntarjoajan tiloissa ja asiakas maksaa ainoastaan käytetyistä resursseista. Asiakkaan ei siis tarvitse huolehtia oman fyysisen palvelinlaitteiston ylläpidosta lainkaan ja resursseja on aina saatavilla.[7]

Käytännössä palvelinvirtualisointi voidaan toteuttaa kahdella eri tavalla. Virtualisointiohjelmisto, josta käytetään nimitystä hypervisor, voidaan asentaa palvelimessa olevan käyttöjärjestelmän päälle (isännöity) tai se voidaan asentaa suoraan fyysiseen laitteistoon (natiivi), jolloin yksi ylimääräinen kerros poistuu ja sen päälle on mahdollista asentaa useita eri käyttöjärjestelmiä. Isännöityä virtualisointitapaa kutsutaan monessa yhteydessä käyttöjärjestelmän virtualisoinniksi. Suoraan laitteistoon asennettavia virtualisointiohjelmistoja ovat esimerkiksi VMwaren ESXi, Microsoft Hyper-V, Citrix XenServer ja KVM. Jos taas virtualisointi halutaan toteuttaa käyttöjärjestelmän päälle, ovat sopivia ohjelmistoja esimerkiksi VMware Workstation ja VirtualBox. Kuvassa 2 on esitetty natiivin ja isännöidyn palvelinvirtualisoinnin erot. Kuten kuvasta näkee, on natiivissa palvelinvirtualisoinnissa virtualisointiohjelmisto asennettu suoraan fyysiselle laitteistolle ja virtualisointiohjelmistoa rajapintana käyttäen voidaan sen päälle asentaa eri käyttöjärjestelmiä käyttäjän tarpeiden mukaan. Isännöidyssä palvelinvirtualisoinnissa taas fyysiseen laitteistoon on asennettu ensin käyttöjärjestelmä, jonka päälle taas on asennettu virtualisointiohjelmisto ja sen päälle taas halutut käyttöjärjestelmät.



Kuva 2: Natiivin ja isännöidyn virtualisointiohjelmiston erot. [7]

3.2 Työpöydän virtualisointi

Työpöydän virtualisoinnilla tarkoitetaan ohjelmistoteknologiaa, jonka avulla voidaan erottaa työpöytäympäristö ja siihen liittyvä ohjelmisto toisistaan. Käytännön esimerkkinä tämä voi tarkoittaa sitä, että palvelinlaitteistolle asennettua käyttöjärjestelmää on mahdollista käyttää tietokoneella, tabletilla tai älypuhelimella verkon kautta. Työpöydän virtualisointi toimii siis asiakas-palvelin mallin perusteella. Asiakas on tässä tapauksessa tietokone, jota kutsutaan thin clientiksi. Thin clientillä tarkoitetaan laitetta, jossa laitteen resurssit ovat rajatut ja isoimmat laskentatehoa vaativat suoritukset tekeekin palvelin, jolloin thin clientin tärkeimmäksi tehtäväksi jää periaatteessa vain näyttää mitä palvelinkoneella suoritettu ohjelma on tehnyt. Asiakkaan päässä olevaa laitetta käyttävä henkilö ei huomaa eroa vaikka ohjelman suorittaakin verkon takana oleva palvelin.

Työpöydän virtualisoinnilla mahdollistetaan nopeasti muutettava ja skaalautuva ympäristö esimerkiksi yrityksiin tai oppilaitoksiin. Ylläpito suurissa organisaatioissa helpottuu sillä ohjelmistoja voidaan päivittää keskitetysti, jolloin säästyy aikaa kun jokaista yksittäistä tietokonetta ei tarvitse päivittää erikseen. Palvelinlaitteiston laitteistoresurssien, kuten muistin ja levytilan päivitys on myös keskitettyä, jolloin virtualisoinnin avulla uusi hankittu levytila voidaan jakaa thin clienttien käyttäjien kesken vaivattomasti. Tietenkin palvelinlaitteisto maksaa enemmän kuin tavalliset palvelimet, mutta kustannuksia säästyy kun thin clientit saavat olla heikkotehoisempia, koska niiden ei tarvitse suorittaa raskaita sovelluksia omalla prosessorillaan, vaan palvelin tekee työn niiden puolesta. Työpöydän virtualisoinnissa on otettava kuitenkin huomioon myös verkon toiminta ja sen luotettavuus. Virtualisoidun työpöydän toimintaan vaikuttaa merkittävästi saatavilla oleva kaistanleveys, keskimääräinen vasteaika ja pakettien hävikki verkossa [8]. Tietysti verkon vaikutus on suurempi riippuen thin clientin käyttöpaikasta,

sillä lähiverkot saadaan usein optimoitua suurempiin nopeuksiin ja lyhyisiin vasteaikoihin melko vaivattomasti, mutta käytettäessä thin clientiä esimerkiksi organisaation sivukonttorilla, tulee verkon toiminta organisaation haarojen välillä ottaa erityisen hyvin huomioon.

Työpöydän virtualisoinnista puhuttaessa on myös tärkeää tietää ero VDI:n (Virtual Desktop Infrastructure) ja Remote Desktop Services -palvelun välillä. VDI:llä tarkoitetaan nimenomaan sitä, että palvelin suorittaa jokaista käyttäjää kohden oman instanssin käyttöjärjestelmästä (esim. Windows 7), mutta Remote Desktop Services -palvelussa jokainen käyttäjä jakaa yhden palvelinohjelmiston käytön (esim. Windows Server 2008 R2). VDI-palvelu voidaan toteuttaa useilla eri ohjelmistoilla, joita ovat esimerkiksi VMware Horizon View, Citrix XenDesktop ja Microsoft Virtual Desktop Virtualization Infrastructure. [8, 9]

3.3 Levytilan virtualisointi

Levytilan virtualisointi on konsepti ja termi jolla kuvataan levytilan kehittyneempää käyttöä sekä yksittäisissä järjestelmissä kuin myös useiden levyjärjestelmien välillä. Kun puhutaan levyjärjestelmästä, on olemassa kaksi eri tapaa virtualisoinnille: lohkojen virtualisointi ja tiedostojen virtualisointi. Lohkojen virtualisoinnissa levyjärjestelmän fyysiset resurssit erotetaan loogisista resursseista ja näin ollen mahdollistetaan pääsy loogisiin resursseihin ilman tarvetta tarkastella fyysisiä resursseja. Lohkojen virtualisointi mahdollistaa näin ylläpitäjille joustavamman tavan jakaa resursseja loppukäyttäjien kesken. Tiedostojen virtualisointi taas poistaa sidokset tiedostojen tasolla olevan datan ja niiden fyysisen sijainnin välillä ja mahdollistaa näin levytilan käytön optimoinnin, palvelimien keskittämisen tiedostojen ja keskeyttämättömän tiedostojen migraation. Viimeisimmällä tarkoitetaan sitä, että tiedostoja voidaan siirtää fyysisesti paikasta toiseen ilman, että käyttöjärjestelmä tai käyttäjä, jolla tiedosto on, huomaa siirtoa ja tiedosto on edelleen käytettävissä.

Levytilan virtualisointi on hyvin usein osa isompaa virtualisointiohjelmistoa (esim. VMware vSphere), jossa virtuaalisia tietokoneita luotaessa tietty osa fyysisestä levyjärjestelmästä osioidaan virtuaalisen tietokoneen käytettäväksi. Sama pätee myös käyttömuistiin ja prosessointitehoon. On kuitenkin olemassa myös pilvipalveluita, jotka keskittyvät ainoastaan levytilan myymiseen palveluna. Esimerkiksi Dropbox tarjoaa asiakkailleen levytilaa pilvessä, jonne voi tallentaa haluamansa tiedostot. Dropboxin taustalla onkin Amazon S3, joka on Amazon Web Services pilvipalvelutarjoajan tuottama levytilaa tarjoava palvelu [10]. Käytännön esimerkkinä levytilan virtualisoinnissa Dropbox on erinomainen. Asiakas näkee tiedoston omalla tietokoneellaan, ikään kuin tiedosto olisi omalla tietokoneella omassa kansiossaan, vaikka se sijaitseekin fyysisesti pilvessä. Myös mahdollisuus ostaa lisätilaa omalle tilille on äärimmäisen nopeaa pilvipalvelun automaation ja nopean provisioinnin ansiosta, sillä kun asiakas tilaa lisä levytilaa, se tulee käytettäväksi välittömäksi. Tilauksen mennessä Dropboxille, järjestelmä

lisää asiakkaan virtuaaliseen järjestelmään välittömästi asiakkaan tilaaman määrän levytilaa palvelimen vapaana olevista fyysisistä resursseista. [11]

3.4 Verkon virtualisointi

Verkon virtualisoinnilla tarkoitetaan laitepohjaisten verkkoresurssien ja ohjelmapohjaisten verkkoresurssien sekä niiden toiminnallisuuden yhdistämistä yhdeksi ohjelmapohjaisesti hallinnoitavaksi kokonaisuudeksi. Verkon virtualisointi on osa sovellusalustan ja resurssien virtualisointia.

Verkon virtualisointi voidaan toteuttaa kahdella eri tavalla, joko ulkoisena verkon virtualisointina (external network virtualization) tai sisäisenä verkon virtualisointina (internal network virtualization). Ulkoisen verkon virtualisoinnin ideana on yhdistää tai erottaa toisistaan yksi tai useampi sisäinen eli paikallinen verkko. Näin voidaan jakaa esimerkiksi organisaation eri tuotantohaarojen verkot erilleen ja pitää tiettyjen verkkojen takana olevat tiedot vain valittujen henkilöiden tai ryhmien saatavilla. Ulkoisen verkon virtualisoinnin tarkoituksena on myös tehostaa verkon toimintaa erityisesti isoissa organisaatioiden verkoissa ja datakeskuksissa. Ulkoinen verkon virtualisointi toteutetaan kahden toisiinsa liitettävän teknologian avulla, jotka ovat VLAN (Virtual Local Area Network) ja verkkokytkimet. Juuri VLANin ja kytkimien avulla ylläpitäjä voi muodostaa haluamansa virtuaalisen verkon olemassa olevan fyysisen verkon resursseilla. Ylläpitäjä voi siis jakaa fyysisen verkon useampiin osiin tai yhdistää fyysisesti erilliset verkot yhtenäiseksi virtuaaliseksi verkoksi.

VLAN on erittäin tärkeä osa verkon virtualisointia, joten sitä on syytä tarkastella hieman yksityiskohtaisemmin. VLAN on siis virtuaalinen lähiverkko, jonka avulla OSI-mallin toisen kerroksen eli siirtoyhteyskerroksen avulla voidaan fyysiset verkot jakaa osiin tai yhdistää. VLAN toteutetaan usein kytkimien tai reitittimien avulla käyttämällä niiden ominaisuuksia. Yksinkertaisimmat laitteet osaavat erottaa eri VLANit toisistaan vain eri fyysisten porttien avulla, eli kytkimen portit on ohjelmoitu vastaamaan tiettyä VLANia, jolloin jokainen VLAN tarvitsee oman fyysisen kaapeloinnin. Kehittyneemmät kytkimet ja reitittimet tukevat kuitenkin jo datapakettien merkitsemistä (tagging) niin, että jokaiseen datapakettiin lisätään tieto VLANista ja datapaketti voidaan ohjata oikeaan VLAN-segmenttiin tämän tiedon avulla. Datapakettien merkitsemisen avulla eri VLAN-segmenttien paketit voivat kulkea yksittäistä kaapelia (trunk line) pitkin eteenpäin. Laajoissa verkoissa, joissa eri laitteet sijaitsevat fyysisesti eri paikoissa, VLAN lisäksi yksinkertaistaa verkon topologiaa verkon osioinnin avulla. VLANien käytöstä virtuaalisissa kytkimissä kerrotaan lisää luvun 4 alaluvuissa.

Toinen verkon virtualisoinnin tapa eli sisäinen verkon virtualisointi tarkoittaa sitä, että yksi järjestelmä sisältää yhden tai useampia verkkoja. Tällä tarkoitetaan usein pilvipalveluissa käytettäviä yhdelle isäntälaitteistolle asennettuja useita virtuaalisia tietokoneita, jotka on erotettu toisistaan ja näin ollen tämä yksi järjestelmä sisältää oman virtuaalisen verkkonsa. Yksi virtualisoitu järjestelmä voi sisältää myös useita verkkoja ja näiden verkkojen oleellisin komponentti on virtuaaliset kytkimet, joihin virtuaaliset

tietokoneet kytketään. Sisäinen verkon virtualisointi voidaan toteuttaa joko hypervisorin hallintaohjelmistojen avulla tai vale-rajapintojen avulla eli siis virtuaalisilla verkkoliitännöillä, VNICeillä. VNIC (Virtual Network Inferface Controller) tunnetaan paremmin nimellä virtuaalinen verkkoadapteri ja kuten jokaisessa verkkoon yhdistettävässä fyysisessä tietokoneessa, tulee myös virtuaalisessa koneessa olla sellainen. VNIC määritetään virtualisoinnissa virtuaalisen tietokoneen verkkoliitännäksi jolloin virtuaalisen tietokoneen käyttöjärjestelmä tunnistaa sen samalla tavalla kuin fyysisen verkkoadapterin. Lisäksi VNICin avulla voidaan virtuaalisessa järjestelmässä jakaa yksi fyysinen verkkoadapteri usealle eri virtuaaliselle käyttöjärjestelmälle. Tässä tapauksessa tulee käyttöön kuitenkin myös virtuaaliset kytkimet, joista lisää tulevassa luvussa. Jokaista virtuaalista verkkoadapteria vastaa jokin fyysinen verkkoadapteri, jonka kautta verkkoyhteys toimii eteenpäin. Pilvipalvelinjärjestelmissä käytetään VNICejä virtuaalisesti luoduissa tietokoneissa.

Verkon virtualisointi ei kuitenkaan kokonaisuudessa ole pelkästään sisäistä tai ulkoista verkon virtualisointia vaan ne voidaan yhdistää. Sisäinen verkon virtualisointi voidaan toteuttaa yhden isäntäpalvelimen sisällä ja ulkoinen virtualisointi erilaisilla alla olevia verkkoja yhdistävillä ohjelmistoilla. Verkon virtualisointi on lisäksi tärkeä väline ohjelmistokehittäjille ja laadunvalvojille sillä mahdollisia vikoja ja ohjelmistojen toimintaa voidaan simuloida virtuaalisilla verkoilla hyvin tarkasti esimerkiksi ennen ohjelmiston tai päivityksen julkaisua, jolloin voidaan varmistaa niiden toimivuus halutunlaisessa toimintaympäristössä. [12]

3.5 Virtualisointiin keskittyneet yritykset

Virtualisoinnin kannalta tärkeimpiä ohjelmistojen tuottajia ovat VMware, Microsoft, KVM ja Citrix. VMware on maailman johtava virtualisointiin ja pilvi-infrastruktuuriin keskittynyt yritys. Se perustettiin vuonna 1998 ja aluksi se keskittyi tietokoneiden virtualisointiin siirtyen sitten laajempiin pilvijärjestelmiin ja sitä kautta verkon virtualisointiin. VMwaren tuote isäntäpalvelimen ohjelmistoksi on ESXi-hypervisor. [13]

Microsoft on maailman suurin ohjelmistoalan yritys, joka on alun perin keskittynyt käyttöjärjestelmien tuottamiseen. Microsoft alkoi kuitenkin tarjota myös palvelinohjelmistoja ja tekniikan kehityksen myötä se on lähtenyt mukaan myös pilvijärjestelmien toteuttamiseen. Microsoftin isäntäpalvelin on nimeltään Microsoft Hyper-V ja sen käyttämä ohjelmisto on Windows Server 2012 R2. [14]

KVM (Kernel-based Virtual Machine) on Open Virtualization Alliancen kehittämä Linux-järjestelmään rakennettu tuki virtualisoinnille. Se kilpailee isompien yritysten kanssa lähinnä sen avulla, että se on vapaaseen lähdekoodiin perustuva. Tällä tarkoitetaan sitä, että se on asennettavissa mihin tahansa Linux-käyttöjärjestelmään, mikäli alla oleva laitteisto vaan tukee sen toimintoja. KVM itsessään ei emuloi virtualisoituja tietokoneita, vaan se on tuki ohjelmistolle, jonka avulla virtualisointi voidaan toteuttaa. Ainoa hallintaohjelmisto KVM:lle on tällä hetkellä QEMU, joka on myös vapaaseen lähdekoodiin perustuva. Sen avulla voidaan suorittaa tietokoneiden virtualisointi, mutta

se ei tarjoa lähiverkkojen kannalta oleellista ohjelmallisesti toteutettua virtuaalista kytkintä. Mikäli KVM:n avulla halutaan toteuttaa virtualisoitu verkko, tulee sen lisäksi käyttää esimerkiksi vapaaseen lähdekoodiin perustuvaa Open vSwitchiä, josta kerrotaan lisää luvussa 4.3.[15]

Citrix on palvelin- ja työasemavirtualisointia, verkkoratkaisuja, SaaS-palveluja ja muita pilvipalveluita tarjoava yhdysvaltalainen yritys. Citrix tarjoaa isäntäpalvelimen ohjelmistoksi Citrix XenServer-virtualisointijärjestelmää. Citrix on suurimmaksi osaksi keskittynyt työasemavirtualisointiin ja tarjoaa yrityksille thin-client -ratkaisuja, joissa sovellukset ja työpöydät voidaan jakaa on-demand palveluna mille tahansa laitteelle. Pilvipalveluihin sopiva XenServer-isäntäpalvelinohjelmisto on ilmainen ja se on vapaaseen lähdekoodiin perustuva ohjelmisto. XenServerin lähiverkon virtualisointiin voidaan käyttää vapaaseen lähdekoodiin perustuvaa Open vSwitchiä. [16]

4 PILVIPALVELUIDEN LÄHIVERKOT

Tässä luvussa esitellään VMwaren ja Microsoftin lähiverkkojen tärkeimmät komponentit eli virtuaaliset kytkimet ja niiden ominaisuuksia. Lisäksi esitellään avoimeen lähdekoodiin perustuvan Open vSwitchin toimintaa ja sen ominaisuuksia. Lähiverkkoa tarkastellaan pääasiassa virtuaalisen verkon puolelta. Fyysinen toteutus verkolle on aina taustalla, mutta tärkeimpänä pilvipalvelun kannalta ovat kuitenkin virtuaalisen lähiverkon kytkimet ja niiden ominaisuudet.

4.1 VMware ja lähiverkot

VMware on virtualisointiohjelmistoja tarjoava yritys. Se on alun perin kehittänyt tietokoneen virtualisointiin liittyviä ohjelmistoja ja laajentanut toimintaansa pilvipalveluiden myötä myös verkon virtualisointiin. VMwaren lähestymistapa verkon virtualisointiin on melko suljettu, sillä se on kehittänyt tuotteensa niin, että ne sisältävät kaiken tarvittavan toiminnallisuuden itsessään. Lisäksi ne sisältävät lisäominaisuuksia, joiden avulla toimintaa voidaan tehostaa. VMware tarjoaa erilaisia lisenssivaihtoehtoja, joiden hinnat ja ominaisuudet kasvavat suhteessa toisiinsa. Esimerkiksi luvussa 4.1.3. esitelty dvSwitch vaatii kalleimman lisenssin, jotta sitä voi käyttää. Tämä saattaakin olla ongelma joillekin asiakkaille, sillä suuret lisenssimaksut houkuttelevat tutkimaan vaihtoehtoja VMwaren ratkaisujen tilalle. VMwaren ratkaisut virtuaalisen lähiverkon osalta on esitelty seuraavaksi.

4.1.1 vCloud Director ja vCenter Server

VMware vCloud Director on VMwaren virtuaalisen pilviympäristön hallintaan suunniteltu ohjelmisto. vCloud nimitystä käytetään kuvaamaan kokonaisuutta, johon kuuluu yksi tai useampia vCenter Servereitä ja näin ollen kokonaisia pilviympäristöjä. Jotta virtualisoitua infrastruktuuria voidaan hallita, tulee siis pilvijärjestelmässä olla vCenter Server -palvelin, jolla on pääsy pilvijärjestelmän tietokantaan. vCenter Server on myös pilviympäristön hallintaan käytettävä palvelinohjelmisto ja se on toiminut pääasiallisena hallintaohjelmistona ennen vCloud Directorin julkaisua. vCenter Serveriä voidaan siis käyttää myös hallintaan, mutta vCloud Director toimii hierarkkisesti vCenter Serverin yläpuolella ja sen avulla on mahdollista hallita useita vCenter Servereitä, mikä taas mahdollistaa datakeskusten jaottelun organisaatiokohtaisesti. vCenter Server toimii siis tavallaan vCloud Directorin ja ESXi-isäntäpalvelimen välissä, välittää vCloud Directorin komennot eteenpäin ja on juuri tämän yhteyden vuoksi välttämätön komponentti joko vCloud Directoria käytettäessä tai ilman sitä.

Tärkein ominaisuus vCloud Directorissa on se, että sen avulla pilvipalveluntarjoajat voivat luoda asiakkailleen tunnukset ja sallia heidän käyttää vCloud Directoria hallitsemaan juuri tiettyä osaa koko järjestelmästä. Tunnusten avulla henkilöille voidaan antaa tiettyjä oikeuksia ja asiakkaat näkevät ainoastaan tilaamansa palvelun, vaikka sen rinnalla toimisi useita eri asiakkaiden pilvipalvelimia. vCloud Directorin avulla asiakas pystyy nopeasti provisioimaan ja hallitsemaan omia pilvipalvelimiaan välittämättä siitä, millä rautapohjaisella ratkaisulla pilvipalvelu on toteutettu.

vCloud Directorissa on myös mahdollisuus käyttää vAppeja. vAppit ovat valmiita virtuaalisia tietokoneita tai virtuaalisia tietokoneryhmiä. Ne siis sisältävät valmiiksi konfiguroituja asetuksia ja niiden avulla provisiointi nopeutuu ja helpottuu. Käyttäjät voivat itse luoda omia tai käyttää valmiiksi tehtyjä vAppeja. Esimerkiksi vShield Edge, joka esitellään luvussa 3.3.7, voidaan luoda automaattisesti vAppien avulla. [17]

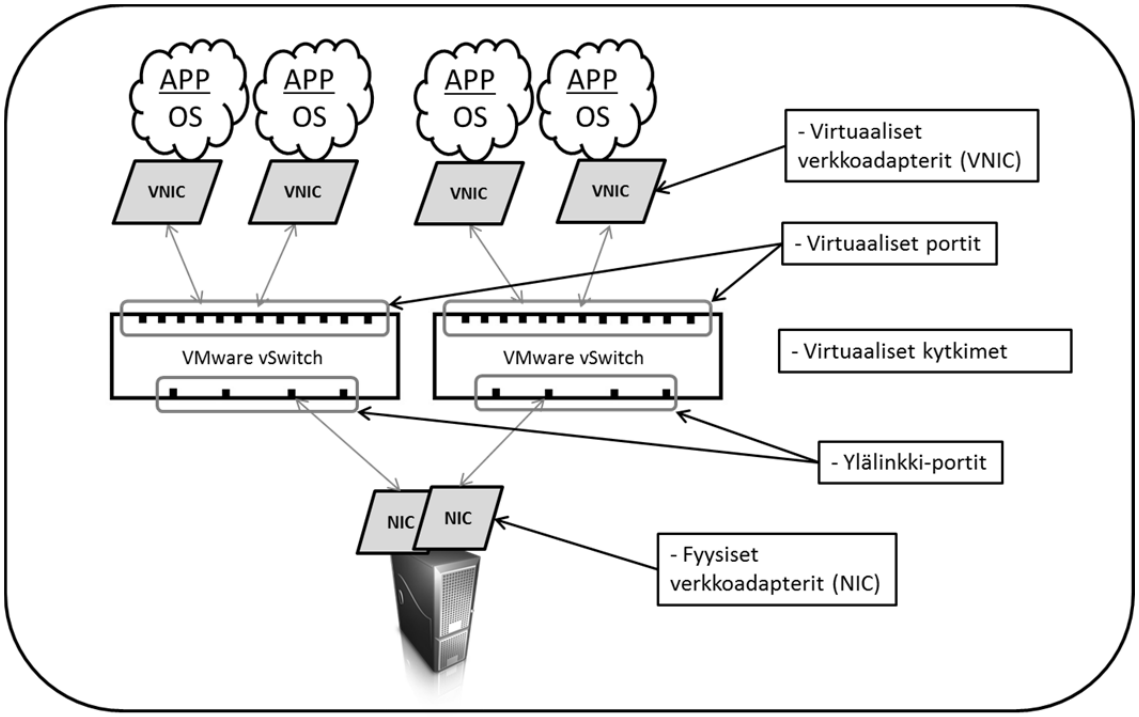
4.1.2 VMware vSwitch

VMware on tietokoneiden virtualisoinnin ohella toteuttanut myös verkon virtualisointia. VMwaren verkon virtualisoinnin avulla on mahdollista muodostaa monimutkaisiakin verkkoja ja integroida ne valmiiseen fyysiseen verkkoon. Verkon virtualisointi toteutetaan ESXi-isäntäpalvelimissa ja niitä hallitaan vCenterin Serverin avulla. Verkkoja voidaan myös hallita vCloud Directorin avulla, joka on koko datakeskuksen hallinnointiin käytettävä ohjelmisto ja jota voivat käyttää niin pilvialustan ylläpitäjät kuin myös loppukäyttäjät eli pilvipalvelun asiakkaat. Käytännössä virtuaaliset verkot toteutetaan virtuaalisilla kytkimillä, jotka ovat vSwitch (virtual switch) ja dvSwitch (distributed virtual switch). Verkon virtualisoinnin avulla voidaan verkot toteuttaa vastaavalla tavalla kuin perinteisillä verkkoratkaisuilla ja näiden verkkojen avulla voidaan luoda verkkoja yhden ESXi-isäntäpalvelimen sisällä, eli yhden isäntälaitteiston virtuaalisten tietokoneiden välille, tai useiden eri ESXi-isäntäpalvelinten välille. Verkkoja voidaan tehdä tuotantoon tai kehittämistä ja testaamista varten. Yksi virtualisoidun verkon eduista on, että virtuaaliset tietokoneet voivat kommunikoida keskenään virtuaalisten kytkinten avulla käyttämällä samoja protokollia kuin käytettäessä fyysisiä kytkimiä, jolloin ei ole tarvetta lisätä ylimääräisiä kytkimiä verkkototeutukseen. Lisäksi virtuaaliset kytkimet tukevat VLAN-teknologiaa, joka esiteltiin luvussa 3.1.4.

Kuten luvussa 3.1.4. on mainittu, jokaisella virtuaalisella tietokoneella on VNIC eli virtuaalinen verkkoadapteri, jolla on oma MAC-osoite ja IP-osoite. Oma MAC- ja IP-osoite tekevät virtuaalisesta tietokoneesta vastaavan kuin fyysisestä tietokoneesta, jolloin virtuaalisella tietokoneella on verkon kannalta vastaavat ominaisuudet kuin fyysisellä tietokoneella ja se voi liikennöidä vastaavalla tavalla kuin fyysinen tietokone. Tämän lisäksi virtuaaliset verkot sisältävät ominaisuuksia, joita ei ole mahdollista toteuttaa fyysisissä verkoissa kuten virtuaalisten kytkinten virheettömyyden varmistaminen.

Virtuaalisten verkkojen avainkomponentit ovat siis virtuaaliset verkkoadapterit virtuaalisissa tietokoneissa ja virtuaaliset kytkimet, jotka käytännössä sijaitsevat ESXi-isäntäpalvelimissa. Virtuaalisilla kytkinten avulla yksittäiset virtuaaliset tietokoneet

voidaan yhdistää toisiinsa ja ESXi-isäntäpalvelin voidaan yhdistää ulkopuoliseen verkkoon, jolloin esim. Internet-yhteys välittyy ESXi-isäntäpalvelimen kautta virtuaalisille tietokoneille. Kuvan avulla (Kuva 4) on havainnollistettu virtuaalisen verkon topologiaa ja kuvassa näkyvät komponentit esitellään seuraavissa luvuissa. [18, s. 3]



Kuva 3: Virtuaalisen verkon topologian ja komponenttien esittely.

Virtuaaliset verkkoadapterit

Virtuaaliset verkkoadapterit virtuaalisille tietokoneille ovat: vmxnet, vlance ja e1000. Vmxnet on paravirtualisoitu - eli se tiedostaa toimivansa virtualisoidussa ympäristössä - verkkoadapteri, joka on suunniteltu korkeaa suorituskykyä varten. Se on myös joustava, joten se toimii lähes kaikkien virtuaalisen tietokoneen käyttöjärjestelmien ja virtualisoidun ympäristön lisäominaisuuksien kanssa. Vmxnet vaatii kuitenkin VMware Tools -lisäominaisuuden asennuksen virtuaalisen tietokoneen käyttöjärjestelmään. Vmxnetistä on lisäksi kolme eri versiota: vmxnet, vmxnet 2 ja vmxnet 3. Vmxnet 2 on päivitetty versio vmxnet -adapterista. Se mahdollistaa jumbo-kehysten (jumbo frames) ja hardware offloadin käytön suorituskyvyn parantamiseksi. Vmxnet 2 -adapteri tukee kuitenkin vain tiettyjä virtuaaliseen tietokoneeseen asennettavia käyttöjärjestelmiä. Vmxnet 3 on seuraavan sukupolven verkkoadapteri, joka kuitenkaan nimestään huolimatta ei ole kytköksissä vmxnet- tai vmxnet 2 -adaptereihin. Se kuitenkin sisältää samat ominaisuudet kuin vmxnet 2 -adapteri ja vielä useita lisäominaisuuksia, kuten IPv6-offloads ja multiqueue-tuen. Lisäksi vmxnet 3 -adapteri voidaan asentaa useammille käyttöjärjestelmille kuin vmxnet 2 -adapteri. Vlance -adapteri taas on emuloitu versio AMD:n vanhemmasta 10 Mbps verkkoadapterista. Se tukee useimpia 32-bittisiä virtuaalisen tietokoneen käyttöjärjestelmiä, mutta ei Windows Vistaa tai sitä uudempia versioita Windowsista. Vlancen etu on, että se on heti käyttövalmis eli se ei vaadi VMware

Tools lisäosan asentamista. E1000 -adapteri on emuloitu versio Intelin Gigabit Ethernet -verkkoadapterista ja se tukee useampia käyttöjärjestelmiä kuin vlance. [19]

Virtuaalisten verkkoadaptereiden tapauksessa on ymmärrettävä, että niissä nopeus- ja duplex-asetukset eivät ole oleellisia kuten fyysisten verkkoadaptereiden tapauksessa. Tämä johtuu siitä, että virtuaalisissa verkkoadaptereissa kaikki datan siirto tapahtuu ESXi-isäntäpalvelimen käyttömuistissa eli RAMissa, jolloin se tapahtuu lähes välittömästi ilman viivettä sekä ilman mahdollisuuksia pakettien törmäyksiin tai muihin viestitykseen liittyviin virheisiin. Lisäksi virtuaaliset verkkoadapterit ovat vain ja ainoastaan OSI-mallin siirtoyhteyskerroksen adaptereita. [18, s. 4]

Virtuaalisten kytkinten toiminta

Virtuaalinen kytkin koostuu useista eri toiminnallisuuksista. Sen päätoiminnot ovat seuraavat: siirtoyhteyskerroksen eteenpäinohjaus (Layer 2 forwarding engine), VLAN-merkintä, -purku ja -suodatusyksiköt sekä siirtoyhteyskerroksen turvallisuus, tarkistussumma ja segmentointi-yksiköt. VLAN-merkintä, sen purku ja suodatus esitetään seuraavassa kappaleessa ja siirtoyhteyskerroksen turvallisuuteen liittyvät asiat kappaleessa ”Virtuaalisen kytkimen siirtoyhteyskerroksen tietoturva”. Segmentointi-yksiköillä tarkoitetaan kytkimen ominaisuutta segmentoida TCP/IP-paketit pienempiin osiin. Segmentointi voidaan määrätä tehtäväksi joko ESXi-isäntäpalvelimen toimesta tai virtuaalisen tietokoneen verkkoadapterin toimesta, jolloin säästetään ESXi-isäntäpalvelimen prosessointitehoa.

Siirtoyhteyskerroksen eteenpäinohjauksella tarkoitetaan varsinaista kytkimen toiminnallisuutta. Se siis ohjaa siirtoyhteyskerroksen paketit oikeaan paikkaan prosessoimalla Ethernet-kehyksen otsakkeen. Se ei siis tutki muita osia kehyksestä kuin otsakkeen ja toimii täysin erillisenä, eli on tietämätön muista toiminnallisuuksista, kuten fyysisten verkkoadaptereiden eroista tai virtuaalisten verkkoadaptereiden emulointieroista. Tämä on modulaarinen tapa toteuttaa kytkin ohjelmallisesti ja virtuaaliset kytkimet ovat toteutettu näin, jotta toimintaa parantavien muutosten ja mahdollisten päivitysten tekeminen jatkossa on helpompaa niin VMwarelle kuin myös ulkopuolisille kehittäjille. Kun virtuaalinen kytkin luodaan, ESXi-isäntäpalvelin lataa ainoastaan tarvittavat komponentit jotka tarvitaan toimivaan yhteyteen. Näin ollen ylimääräiset moduulit ja toiminnallisuudet jäävät pois ja järjestelmän käsiteltäväksi tulevat vain välttämättömät komponentit, jolloin järjestelmän suorituskyky pysyy mahdollisimman tehokkaana. ESXi-isäntäpalvelin valitsee komponentit riippuen tehdyistä konfiguraatiovalinnoista sekä käyttöön tulevasta fyysisestä sekä virtuaalisesta verkkoadapterista. [18, s. 4]

Virtuaalisen ja fyysisen kytkimen samankaltaisuudet

Virtuaalinen kytkin on monella tapaa samankaltainen kuin fyysinen kytkin. Kuten fyysinen kytkin, myös virtuaalinen kytkin sisältää seuraavat ominaisuudet ja toiminnallisuudet: sisältää osoitetaulun (MAC-osoite ja sitä vastaava portti), tutkii jokaisen tulevan kehyksen kohteen MAC-osoitteen ja ohjaa sen eteenpäin oikeaan porttiin tai portteihin

ja välttelee tarpeettomia eteenpäinohjauksia eli toisin sanoen se on älykkäämpi laite kuin keskitin (hub).

Virtuaalinen kytkin tukee myös VLAN-segmentointia porttitasolla. Tällä tarkoitetaan, että jokainen portti voidaan konfiguroida kahdella eri tavalla. Portti voidaan konfiguroida yhdellä VLANilla. Tätä kutsutaan virtuaalisen kytkimen merkitsemiseksi. Fyysisten kytkinten tapauksessa tällä tavalla konfiguroitua porttia kutsutaan access-portiksi. Vaihtoehtoisesti portti voidaan konfiguroida vastaamaan useampia VLANeja ja tätä kutsutaan virtual guest taggingiksi eli virtuaalisen vieraan merkinnäksi. Fyysisten kytkinten tapauksessa tällä tavalla konfiguroitua porttia kutsutaan trunk-portiksi. Virtuaalisen vieraan merkitsemisessä kehyksiin lisätyt VLAN-merkit jätetään kehykseen eikä niitä poisteta, kuten virtuaalisen kytkimen merkinnässä. Tällöin kehyksissä oleva VLAN-tieto välittyy myös seuraavalle laitteelle, joka käsittelee kehyksiä. Virtuaalinen kytkin voidaan konfiguroida porttikohtaisen tavan lisäksi myös kokonaisuutena, jolloin kytkimeen tehdyt asetukset tulevat voimaan kaikissa porteissa.

Virtuaalinen kytkin, kuten useat fyysisetkin kytkimet, tukee portin peilausta. Tämä tarkoittaa siis sitä, että tiettyyn porttiin lähetetyt paketit kopioidaan ja lähetetään peilattuun porttiin. Peilauksen avulla voidaan paketteja tutkia helpommin ja selvittää esimerkiksi vikoja pakettikaappausten avulla tai valvoa verkon toimintaa monitorointiohjelmistoilla kuten IDS (intrusion detection system). VMwarella tätä toimintoa kutsutaan promiscuous modeksi. Portin peilausta käytetään tämänkin työn myöhemmässä kappaleessa verkon toiminnan tutkimiseen esimerkiksi simuloitujen vikatilanteiden sattuessa. [18, s. 4-5]

Virtuaalisen ja fyysisen kytkimen eroavaisuudet

Vaikka virtuaalinen kytkin on toiminnaltaan hyvin samankaltainen kuin fyysinen kytkin, on niissä kuitenkin pieniä eroja. Ensinnäkin virtuaaliset kytkimet luodaan ESXi-isäntäpalvelimessa, joten virtuaalinen kytkin tietää jokaisen kytkimeen liitetyn virtuaalisen tietokoneen MAC-osoitteen ja VMkernelin portit kun virtuaaliset laitteet rekisteröidään ESXi-isäntäpalvelimeen. VMkernel on rautapohjaisen alustan ja virtuaalisten tietokoneiden välillä toimiva ydinohjelmisto, jonka tehtävä on esimerkiksi ohjata prosessoreita ja luoda rajapinta virtuaalisten ja fyysisten komponenttien välille. Tämän vuoksi virtuaalisen kytkimen ei ole tarvetta oppia tai lisätä MAC-osoitteita sen osoitetauluun tai suorittaa IGMP-snooping toimintoa, jotta se saisi selville liittymiset ryhmälähetykseen. Virtuaalinen kytkin lisäksi hylkää kaikki paketit, joiden MAC-kohdeosoite ei vastaa yhtäkään siihen kytkettyä virtuaalista tietokonetta, mikä lisää tietoturvaa estämällä MAC-flooding -hyökkäykset. MAC-flooding -hyökkäyksellä tarkoitetaan sitä, että ulkopuolinen yrittää asettaa kytkimen MAC-osoitetauluun uusia MAC-osoitteita niin paljon, että vanhat muistissa olleet MAC-osoitteet poistuvat taulusta ja kytkin toistaa täten näihin menetettyihin MAC-osoitteisiin kohdennetut kehykset kaikkiin portteihin. Lisäksi virtuaalinen kytkin ei ohjaa ylälinkki-porttiin tulleita tietoja koskaan ulospäin ylälinkki-portista, mikä tarkoittaa samalla sitä, että useita virtuaalisia kytkimiä ei voida kytkeä toisiinsa. Useiden virtuaalisten kytkimien liittäminen yhteen ei ole tarpeellista, sillä yh-

teen virtuaaliseen kytkimeen on mahdollista asettaa huomattavasti suurempi määrä portteja kuin fyysiseen kytkimeen. Virtuaalisen kytkimen ylälinkki-porttiin tulleet kehykset hylätään, mikäli ne eivät täsmää yhteenkään virtuaalisen tietokoneen MAC-osoitteeseen tai kohdeportteihin. Ylälinkki-porteista kerrotaan tarkemmin ”Ylälinkki-portit” -luvussa. Ylälinkki-porttien hylkäysperiaate estää luuppien muodostumisen virtuaaliseen verkkoon. Luupit eivät siis periaatteessa ole mahdollisia virtuaalisten kytkinten tapauksessa. Tämä ei kuitenkaan täysin pidä paikkaansa, sillä luomalla virtuaalisen tietokoneen kahdella virtuaalisella verkkoadapterilla ja konfiguroimalla näiden asetukset tietyllä tavalla, on mahdollista muodostaa luuppi virtuaaliseen verkkoon. Tämä on kuitenkin äärimmäisen hankalaa saada aikaiseksi vahingossa, joten käytännössä virtuaaliset verkot ovat luupittomia. Ylälinkki-porttien hylkäysperiaate ja siten luupittomuus mahdollistaa myös sen, että spanning tree -protokollaa (SPT) ei tarvita. Spanning tree -protokolla on tehty nimenomaan estämään luuppien muodostuminen lähiverkkoihin. Sen perusperiaate on estää siltayhteyksien muodostuminen ja tämän jälkeen lähetettävien broadcast-lähetysten eteneminen. [18, s. 5; 20]

Virtuaalisen kytkimen eristäytyneisyys

Kuten edellisessä kappaleessa mainittiin, yhdelle ESXi-isäntäpalvelimelle luotuja virtuaalisia kytkimiä ei ole mahdollista kytkeä toisiinsa. Rajoitus ei sinänsä ole merkittävä, sillä virtuaalisessa kytkimessä voi olla portteja 1016 kappaletta. Lisäksi yhdellä ESXi-isäntäpalvelimella voi olla enintään 248 virtuaalista kytkintä. Tärkeä huomio on kuitenkin se, että yhdelle ESXi-isäntäpalvelimelle luotujen virtuaalisten kytkinten porttien lukumäärä on maksimissaan 4096. Kytkinten yhdistämisen rajoituksen avulla saavutetaan seuraavat hyödyt: koska virtuaalinen kytkin mahdollistaa laajan verkon luomisen vain yhden kytkimen avulla suuren porttilukunsa ansiosta, ei ole myöskään tarvetta sarjoittaa kytkimiä toisiinsa ja näin vältytään myös tekemästä huonoja kytkimien yhdistämisiä. Toiseksi, koska virtuaaliset kytkimet eivät voi jakaa fyysistä verkkoadapteria, vältytään lähiverkkoon syntyviltä luupeilta ja vastaavan konfiguroinnin aiheuttamilta mahdollisilta vuodoilta. Lisäksi jokaisella virtuaalisella kytkimellä on oma osoitetaulunsa, jonka mukaan kytkin toimii ja kaikki kehykset, joiden osoitetiedot eivät täsmää osoitetauluun, hylätään. Tästä voidaan päätellä myös se, että vaikka toisella ESXi-isäntäpalvelimella olevassa virtuaalisessa kytkimessä olisi kohdeosoitetta vastaava tieto, niin kehys hylätään silti, sillä eri ESXi-isäntäpalvelimilla olevat virtuaaliset kytkimet ovat eristettyjä toisistaan. On kuitenkin huomattava, että kahden virtuaalisen kytkimen yhdistäminen onnistuu toisiinsa, mikäli kahden virtuaalisen kytkimen ylälinkki-portit kytketään toisiinsa tai mikäli virtuaaliset kytkimet sillataan toisiinsa virtuaaliselle tietokoneelle asennettavan sovelluksen avulla. Ylälinkki-porttien kytkeminen toisiinsa ei kuitenkaan onnistu ilman fyysiseen kytkimeen tehtyä konfiguraatiota, joten tämän tilanteen syntyminen vahingossa on hyvin epätodennäköistä. Mikäli nämä tilanteet kaikesta huolimatta tapahtuisivat, virtuaalinen kytkin joutuisi alttiiksi samoille ongelmille kuin fyysisen kytkin joutuisi vastaavissa tapauksissa. [18, s. 5]

Virtuaaliset portit

Virtuaaliset portit ovat virtuaalisen kytkimen portteja, joihin virtuaalisten tietokoneiden virtuaaliset verkkoadapterit kytketään. Kuten edellisessä kappaleessa jo sivuttiin, virtuaalisia portteja voi olla yhdessä ESXi-isäntäpalvelimessa yhteensä 4096 kappaletta ja virtuaalisia kytkimiä voidaan luoda yhdelle ESXi-isäntäpalvelimelle 248 kappaletta. Rajoituksena on kuitenkin vielä lisäksi, että virtuaalisia portteja voi olla yhdessä kytkimessä 1016 kappaletta. Näin ollen neljällä virtuaalisella kytkimellä saadaan kaikki mahdolliset portit yhden ESXi-isäntäpalvelimen tapauksessa käyttöön.

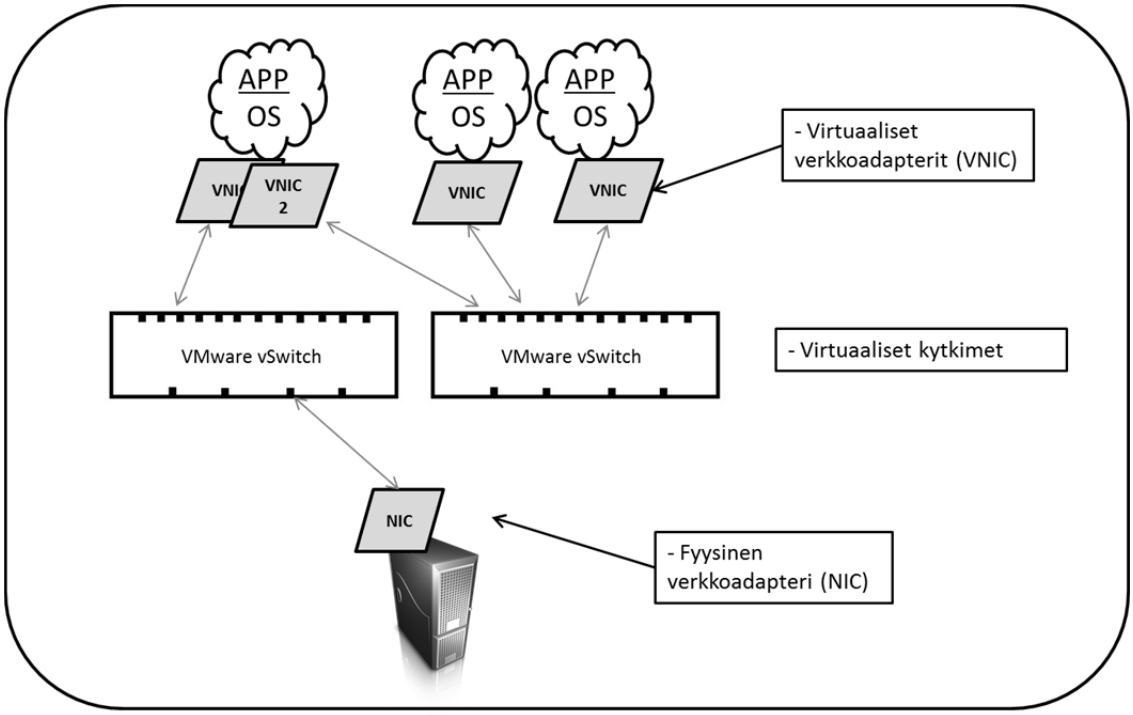
ESXi-isäntäpalvelimen virtuaalisen kytkimen portit tietävät varmasti, mitkä ovat siihen liitettyjen virtuaalisten verkkoadaptereiden MAC-osoitteet ja niitä vastaavat portit. Varmalla tiedolla tarkoitetaan sitä, että virtuaalisten verkkoadaptereiden MAC-osoitteiden hallinta on itse ESXi-isäntälaitteella ja esimerkiksi virtuaaliset tietokoneet eivät voi niitä itse muuttaa. Näin ollen kytkimen ei tarvitse oppia mitään verkon puolelta eikä niiden tarvitse välittää eteenpäin osoitetaulua. Virtuaalisen ja fyysisen kytkimen ero erityisesti porttien kannalta on juuri tässä, sillä luottamuksellisella kytkimen tiedolla tarkoitetaan virtuaalisen kytkimen tapauksessa sitä, että siihen kytkettyjen virtuaalisten tietokoneiden MAC-osoitteet sijaitsevat konfiguraatiotiedostossa, johon itse virtuaalisella tietokoneella ei ole pääsyä. Näin ollen virtuaalinen kytkin tietää tarkalleen, mitä porttia vastaa mikäkin MAC-osoite.

Virtuaaliset portit aktivoituvat kun virtuaalinen tietokone kytketään päälle, verkkoyhteys virtuaaliseen tietokoneeseen kytketään päälle erillisesti tai kun virtuaalinen tietokone kytketään osaksi VMotion toimintoa. Lisäksi virtuaalinen verkkoadapteri päivittää virtuaalisen kytkimen portin MAC-suodatustiedot eli virtuaalisen kytkimen osoitetaulut ensiasennuksessa tai silloin kun ne muuttuvat. Virtuaalinen portti sisältää myös tietoturvaa, sillä asetuksia muuttamalla on mahdollista kytkeä portti toimimaan esimerkiksi niin, että se hylkää kaikki paketit jotka rikkovat siirtoyhteyskerroksen tietoturvasääntöjä. Esimerkiksi MAC-spoofing voidaan kieltää, jolloin kaikki tätä sääntöä rikkovat paketit hylätään. MAC-spoofingissa käyttäjä voi muuttaa oman verkkoadapterinsa MAC-osoitteen, joka normaalisti on uniikki, vastaamaan mitä tahansa haluamaansa MAC-osoitetta. [18, s. 5]

Ylälinkki-portit

Ylälinkki-portit ovat yhteydessä fyysisiin verkkoadaptereihin, jotka muodostavat yhteyden virtuaalisen ja fyysisen verkon välille. Fyysiset verkkoadapterit muodostavat yhteyden ylälinkki-portteihin kun ne asennetaan tai silloin kun virtuaalisen kytkimen ryhmityssääntöjä on konfiguroitu. Kaikissa virtuaalisissa kytkimissä ei ole ylälinkki-porttia, koska niiden ei haluta olevan yhteydessä suoraan fyysiseen verkkoon. Tällainen tilanne voi olla esimerkiksi silloin, kun palomuurina toimii virtuaalinen tietokone ja näin ollen kaiken datan halutaan kulkevan sen kautta muille virtuaalisen sisäverkon laitteille. Tämänkaltaisissa tapauksissa ylälinkki-portti on käytössä vain virtuaalisen palomuuriohjelmiston sisältävän tietokoneen ja fyysisen verkon välisessä kytkimessä ja palomuuritietokone sisältää kaksi virtuaalista verkkoadapteria joista toinen on yhdistetty rinnak-

kaiseen virtuaaliseen kytkimeen. Seuraavassa kuvassa (Kuva 5) on havainnollistettu tämä tilanne paremmin. Ylälinkki-portit yhdistävät kytkimen ja fyysisen verkon toisiinsa asennusvaiheessa tai kun niiden tiedot päivittyvät konfiguraatiomuutoksissa. [18, s. 6]



Kuva 4: Virtuaalinen verkko jossa vain toisessa kytkimistä ylälinkki-portti. [18, s. 6]

Porttiryhmät

Porttiryhmät ovat tärkeä osa VMwaren pilvipalvelun infrastruktuuria. Ne eivät kuitenkaan täysin vastaa fyysisten kytkinten porttiryhmiä vaan niitä voi ajatella pikemminkin valmiina porttien asetusmalleina, jotka sisältävät tietyt asetukset. Lähin fyysisen kytkimen vastaava ominaisuus olisi joissakin Ciscon kytkimissä oleva SmartPort-ominaisuus. Yksi ESXi-isäntäpalvelin voi sisältää korkeintaan 512 porttiryhmää.

Porttiryhmät ovat erityisen tärkeitä VMotion lisäominaisuudelle. Porttiryhmien avulla voidaan määrittää tietyt vaatimukset, joilla virtuaalisen tietokoneen tulee toimia jokaisella ESXi-isäntäpalvelimella, jolla se saattaa VMotionin vuoksi olla sijoitettuna. Porttiryhmät ovat käyttäjän nimeämiä objekteja, jotka sisältävät riittävän määrän konfiguraatioasetuksia, jotta saavutetaan jatkuva ja johdonmukainen yhteys virtuaalisille verkkoadaptereille. Porttiryhmät sisältävät seuraavat tiedot: virtuaalisen kytkimen nimi, VLAN-tiedot ja säännöt merkitsemiselle ja suodatukselle, ryhmittämissäännöt (teaming policy), siirtoyhteyskerroksen tietoturva-asetukset sekä liikenteen muokkaukseen liittyvät parametrit (traffic shaping parameters). Lyhyesti sanottuna porttiryhmät sisältävät kaikki tarvittavat asetukset ja kun virtuaalinen tietokone halutaan liittää kytkimeen, voidaan se tehdä ainoastaan määrittämällä halutun porttiryhmän nimi. Porttiryhmät saattavat sisältää erilaisia asetuksia eri ESXi-isäntäpalvelinten välillä, mutta tärkeintä on, että porttiryhmien avulla virtuaaliselle tietokoneelle tulee yhtenäinen kuva verkosta riippu-

matta siitä millä ESXi-isäntäpalvelimella se toimii eli minkä ESXi-isäntäpalvelimen resursseja se parhaillaan käyttää. Huomioitava asia on, että porttiryhmät eivät välttämättä täsmää VLAN-ryhmien kanssa yhteen. Eli on siis mahdollista ja jopa suotavaa tietyissä tilanteissa tehdä asetukset niin, että useat porttiryhmät vastaavat samoja VLANeja. Tämä voi olla hyödyllistä esimerkiksi tapauksessa, jossa halutaan antaa eri virtuaalisten tietokoneiden ryhmille erilliset fyysiset verkkoadapterit valmiustilaa ja aktiivista liikennöintiä varten, vaikka verkkoadapterit sijaitsevatkin samassa VLANissa. [18, s. 6]

Ylälinkit

Fyysiset verkkoadapterit toimivat ESXi-isäntäpalvelimessa siltana virtuaalisen ja fyysisen verkon välillä ja niitä kutsutaan ylälinkeiksi. Kuten ylälinkki-portit luvussa kerrottiin, ovat näihin ylälinkkeihin liitetyt virtuaaliset portit ylälinkki-portteja. Yhdellä ESXi-isäntäpalvelimella voi olla enintään 32 ylälinkkiä ja ne voivat olla sijoitettu yhteen kytkimeen tai jaettu useamman virtuaalisen kytkimen kesken. Jotta virtuaalisen kytkimen kautta on pääsy useampaan kuin yhteen VLANiin pitää fyysiseen verkkoadapteriin kytketyn fyysisen kytkimen portin olla trunking moodissa. Eli tämän portin tulee päästää läpi useampaan VLANiin lähetetyt kehykset. On myös tärkeää, että virtuaalisesta kytkimestä poistetaan ylimääräiset VLANit sillä ne aiheuttavat ESXi-isäntäpalvelimen ylimääräistä kuormittumista. Tämä johtuu siitä, että ESXi-isäntäpalvelin joutuu käsittelemään kaikkien siihen kytkettyjen VLANien yleislähetys-kehykset. Ylimääräiset VLANit tulee poistaa sekä fyysisestä kytkimestä kuin myös ylälinkistä. Fyysisen kytkimen VLANien poistaminen ei välttämättä ole niin tehokasta kuin ylälinkin puolella, sillä virtuaalisessa kytkimessä ESXi-isäntäpalvelin tietää mitkä virtuaaliset tietokoneet ovat päällä ja mitkä suljettuina kun taas fyysinen kytkin ei tätä tiedosta. Näin ollen virtuaalisen kytkimen puolella VLANien poisto on tehokkaampaa ja antaa paremmat lopputulokset.

Ylälinkkeihin liittyvät myös virtuaaliset porttiryhmät. Eri porttiryhmiin on mahdollista määrittää erilaiset ryhmityskäyttäytymiset. Ryhmittämisellä (teaming) tarkoitetaan sitä, että tiettyyn virtuaaliseen porttiryhmään kuuluvat virtuaaliset tietokoneet jakavat useita ylälinkkejä keskenään. On esimerkiksi mahdollista muuttaa jokaisen ylälinkin tilaa aktiiviseksi tai valmiustilaan eri porttiryhmien kesken, jolloin saavutetaan sekä hyvä linkkien yhteistoiminta (link aggregation) että toimintavarmuus (failover behavior). Ryhmitystila säilytetään jokaisen porttiryhmän tiedossa. Ryhmitystilalla tarkoitetaan sitä tietoa, mikä tietty fyysinen verkkoadapteri juurikin kuljettaa dataa. Ryhmitystilan muuttuminen, eli ylälinkin vaihtuminen toiseksi ylälinkiksi ei näy virtuaalisille tietokoneille varsinaisesti millään tavalla. Virtuaaliset tietokoneet eivät esimerkiksi tiedä milloin toinen ylälinkki on joutunut virhetilaan ja dataa siirretäänkin toisen ylälinkin kautta tai sitä, mitä kautta mikäkin lähetetty kehys kulkee. Kuitenkin siinä vaiheessa kun ryhmittymistila palautuu entiselleen eli esimerkiksi varayhteytenä toimineesta ylälinkistä yhteys palautuu kulkemaan ensisijaiseen ylälinkkiin, verkon tilan muutos on näkyvä virtuaaliselle tietokoneelle. Ylälinkkien ryhmittämisestä kerrotaan tarkemmin kappaleessa ”Fyysisten verkkoadaptereiden ryhmitys”.

Virtuaalinen verkko toimii myös ilman ylälinkkejä. Virtuaalisten tietokoneiden verkkoadapterit voivat keskustella paikallisesti keskenään virtuaalisen kytkimen kautta. Myöskään tilanteessa, jossa virtuaalisessa kytkimessä on ylälinkki, sitä ei käytetä paikalliseen tiedonvälitykseen vaan sen kautta kulkee tieto ainoastaan kun sisäverkosta halutaan siirtyä ulkoverkkoon.

On tärkeää myös huomata, että virtuaalinen kytkin käsittelee eri VLANeja samalla tavoin kuin kahden kytkimen välistä kommunikointia, eli se ei ole sallittua. Virtuaalinen kytkin ei siis salli tiedonsiirtoa kahden eri VLANin välillä, joten mikäli halutaan kahden portin pystyvän kommunikoimaan keskenään, on niiden oltava samassa VLANissa. Mikäli kahden virtuaalisen kytkimen tai VLANin halutaan kommunikoivan keskenään, tulee niiden välinen yhteys toteuttaa ulkoisella sillalla tai reitittimellä. [18, s. 6-7]

Virtuaalisen kytkimen virheettömyys

Virtuaalisten kytkinten tapauksessa kaksi asiaa liittyen niiden virheettömyyteen on erityisen tärkeitä. On tärkeää että verkossa olevat virtuaaliset tietokoneet tai muut solmupisteet eivät vaikuta virtuaalisen kytkimen käyttäytymiseen. ESXi-isäntäpalvelin huolehtii tästä kahdella eri tavalla. Virtuaaliset kytkimet eivät voi oppia verkosta niin, että ne lisäisivät uusia tietoja osoitetauluihinsa. Tämä estää palvelunesto- ja vuotohyökkäysten (leakage-attacks) mahdollisuuden joko suoraan tai niiden tullessa viruksen aiheuttamana sivuvaikutuksena. Lisäksi virtuaaliset kytkimet tekevät yksityisiä kopioita kaikista kehysten tiedoista, joiden perusteella se tekee eteenpäinohjaus- tai suodatuspäätöksiä. Tämä toiminto on äärimmäisen tärkeä ominaisuus ja se on ainoastaan virtuaalisissa kytkimissä. Virtuaalinen kytkin ei kuitenkaan kopioi koko kehystä, sillä se kuluttaisi turhaan ESXi-isäntäpalvelimen resursseja. Eteenpäinohjaus- ja suodatuspäätöksien vuoksi tehtävien kehyksen tietojen kopioinnin avulla ESXi-isäntäpalvelin pitää huolen, että virtuaalisella tietokoneella ei ole pääsyä tärkeisiin tietoihin sen jälkeen kun kehys on ohjattu virtuaaliselle kytkimelle. Toinen tapa jolla virheettömyys taataan on se, että ESXi-isäntäpalvelin huolehtii että tiettyyn VLANiin kuuluvat kehykset eivät joudu muihin VLANeihin. Tämä toteutetaan kahdella eri tavalla. Ensinnäkin VLAN-tieto sijaitsee lähetetyn kehyksen ulkopuolella, joten VLANin suodatus on käytännössä yksinkertainen muuttujan tarkistus. Lisäksi virtuaalisissa kytkimissä ei ole dynaamista trunking-tukea. Dynaaminen trunking ja natiivi VLAN ovat ominaisuuksia joiden avulla hyökkääjä saattaa löytää verkosta heikkouksia ja näin päästä käsiksi verkkoon vuotojen avulla. Tällä ei tarkoiteta sitä, että nämä ominaisuudet olisivat automaattisesti alttiita hyökkäyksille, mutta lisäämällä niihin tietoturvaa lisätään samalla niihin monimutkaisuutta, joka usein johtaa vääriin konfigurointeihin ja näin ollen tietoturvariskeihin. [18, s. 7]

VLANit VMware infrastruktuurissa

VLANit mahdollistavat verkon jakamisen eri loogisiin osiin joko tietokoneryhmien tai kytkimen porttien perusteella niin, että tiettyyn loogiseen osaan kuuluvat laitteet näke-

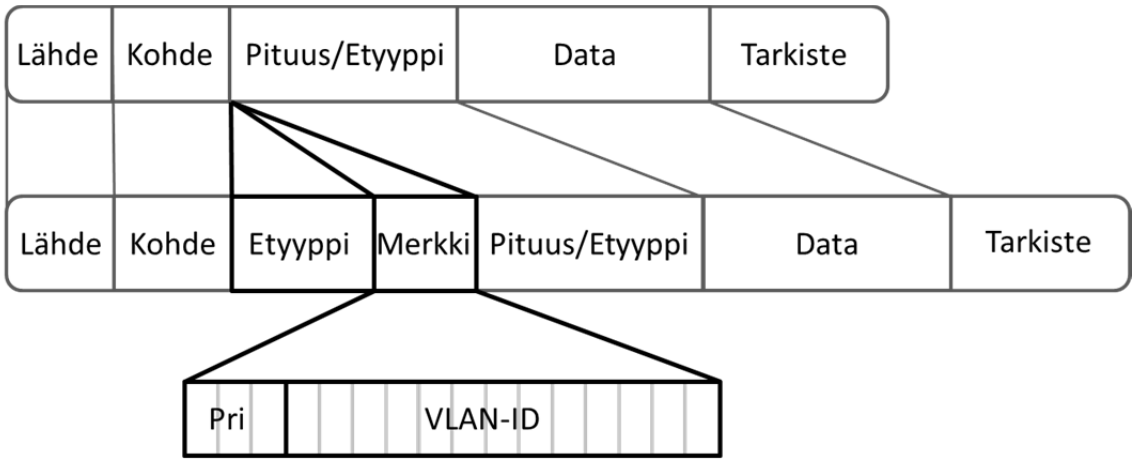
vät toisensa kuin ne olisivat samassa lähiverkossa. Yleislähetys-liikenteen rajaaminen tiettyihin kytkimen portteihin tai loppukäyttäjiin säästää huomattavan määrän liikennöintikapasiteettia ja prosessorin suorituskykyä. Jotta VLANeja voidaan käyttää VMware infrastruktuurissa, tulee jonkin verkon osan merkitä Ethernet-kehykset 802.1Q merkillä eli VLANin standardin mukaisella merkinnällä.

Tämän merkinnän voi tehdä kolmella eri tavalla. Virtual switch tagging (VST mode) eli virtuaalisen kytkimen merkintä on yleisimmin käytetty tapa. Tässä konfiguraatiossa asetetaan yksi porttiryhmä vastaamaan yhtä VLANia ja yhdistetään halutut virtuaalisten tietokoneiden verkkoadapterit tähän porttiryhmään itse virtuaalisen kytkimen sijaan. Tässä tapauksessa virtuaalinen porttiryhmä merkitsee kaikki lähtevät kehykset ja purkaa merkinnät kaikista saapuvista kehyksistä. Samalla porttiryhmä varmistaa, että tietyn VLANin kehykset eivät vuoda toiseen VLANiin. Jos halutaan käyttää tätä tapaa VLAN-merkitsemiseen, tulee fyysisen kytkimen tarjota trunk-linja.

Toinen tapa tehdä VLAN-merkintä on virtual guest tagging (VGT mode) eli virtuaalisen vieraan merkintä. Tällä tavalla toteutettuna virtuaaliseen tietokoneeseen asennettu 802.1Q VLAN trunking -ajuri tekee merkinnän ja se säilyy kulkiessaan virtuaalisen kytkimen läpi ulkoiseen kytkimeen. Tämäkin tapa vaatii trunk-linjan konfiguroinnin fyysiseen kytkimeen.

Kolmas tapa on external switch tagging (EST mode) eli ulkoisen kytkimen merkintä. Tässä tapauksessa VLAN-merkintään käytetään ulkoista kytkintä. Tämä tapa on verrattavissa fyysiseen verkkoon toteutettuun VLAN-merkintään ja se ei useimmissa tapauksista näy millään tavalla fyysisille palvelimille. Tässä konfiguraatiossa ei ole tarvetta trunk-linjalle.

Kuvassa (Kuva 6) on esitetty normaalin Ethernet-kehyksen ja VLAN-merkityn Ethernet-kehyksen otsakkeet. VLAN-merkinnässä otsakkeeseen lisätään 32-bittinen lisätietokenttä. Kuvassa normaali Ethernet-kehyksen otsake on yläpuolella ja VLAN-merkitty otsake alapuolella. [18, s. 7-8]



Kuva 5: Normaalin ja VLAN-merkityn Ethernet-kehyksen otsakkeet. [18, s. 7]

VLAN-merkityn Ethernet-kehyksen otsake sisältää seuraavat lisätiedot: 16-bittisen Ethernet-tyypin eli tunnisteen josta selviää, että kyseessä on VLAN-merkitty kehys, merkintä-kentän, joka taas sisältää 3-bittisen prioriteettikentän, 1-bittisen kanonisen formaatin ilmoituskentän ja 12-bittisen VLAN-tunnisteen, joka sisältää tiedon VLANista johon kehys kuuluu. Prioriteetti-kenttää voidaan käyttää määrittämään kehyksen tärkeys, mikäli halutaan priorisoida liikennettä. Lisäksi VLAN-merkitty otsake sisältää tavalliseen otsakkeen tavoin lähteen ja kohteen MAC-osoitteet, kehyksen pituuden kertovan kentän, hyötykuorma- eli data-kentän ja tarkiste-kentän. VLAN-merkinnässä otsakkeen tiedoista muuttuu ainoastaan tarkiste, joka lasketaan koko otsakkeesta. Muut kentät pysyvät muuttumattomina. [21]

Fyysisten verkkoadaptereiden ryhmitys

VMwaren infrastruktuurissa on mahdollista yhdistää yksi virtuaalinen kytkin useaan fyysiseen verkkoadapteriin ryhmityksen avulla (NIC teaming). Ryhmityksen avulla voidaan yksittäisten, haluttujen tai jopa kaikkien virtuaalisten osapuolien kuormaa jakaa useammalle fyysiselle verkkoadapterille sekä luoda varaväylä liikennöinnille rautapohjaisen vian tai verkkoyhteyden katkeamisen tapahtuessa. Ryhmityssäännöt määritellään porttiryhmien tasolla. Kuorman tasapainottamisesta ja failover-konfiguraatiosta kerrotaan tarkemmin seuraavissa luvuissa. [18, s. 8]

Kuorman tasapainottaminen

Kuorman tasapainottamisen (Load Balancing) avulla voidaan jakaa virtuaalisten tietokoneiden verkkoliikennettä virtuaalisessa kytkimessä usemmalle fyysiselle verkkoadapterille, jolloin saavutetaan suurempi läpäisy kuin yhdellä fyysisellä verkkoadapterilla olisi mahdollista. Kuorman tasapainottaminen voidaan tehdä neljän eri määrityksen mukaan. Ensimmäisen tasapainotustavan mukaan reitti määräytyy alkuperäisen virtuaalisen kytkimen portin mukaan (route based on the originating virtual switch port ID). Näin tehtäessä ylälinkki-portti valitaan sen perusteella mihin kytkimen porttiin liikenne tuli saapuessaan virtuaaliselle kytkimelle. Virtuaalisen portin mukaan toimiva tasapainotus on oletusasetuksena ja yleisin käytetty tapa kuorman tasapainottamiseen. Tätä asetusta käytettäessä tietyltä virtuaaliselta verkkoadapterilta tullut liikenne ohjataan aina samaan fyysiseen verkkoadapteriin, ellei ole tapahtunut vikatilanne, jolloin liikenne ohjautuu varareittinä toimivaan fyysiseen verkkoadapteriin. Vastaukset verkosta saapuvat samaan fyysiseen verkkoadapteriin, koska fyysinen kytkin oppii porttikytköksen. Virtuaalisen portin mukaan toimivan tasapainotuksen avulla liikennekuorma jakautuu tasaisesti fyysisille verkkoadaptereille, mikäli virtuaalisten verkkoadaptereiden määrä on suurempi kuin fyysisten verkkoadaptereiden. On myös huomioitava, että virtuaalinen tietokone ei voi käyttää useampaa kuin yhtä fyysistä verkkoadapteria hyväkseen, mikäli sillä itsellään ei ole kuin yksi virtuaalinen verkkoadapteri. [18, s. 8]

Kuorman tasapainotuksen toisessa vaihtoehdossa ylälinkki eli liikennöintiin käytettävä fyysinen verkkoadapteri valitaan lähteen MAC-osoitteen tiivisteen perusteella. Kuten aikaisemmassakin konfiguroinnissa, myös tässä tilanteessa tietty virtuaalinen

verkkoadapteri liikennöi aina saman fyysisen verkkoadapterin kautta, mikäli kyseessä ei ole vikatilanne, jolloin liikennöinti on ryhmityssääntöjen mukaan siirtynyt toiselle fyysiselle verkkoadapterille. Vastaukset eli saapuva liikenne kulkee myös tämän tietyn fyysisen verkkoadapterin kautta, sillä jälleen fyysinen kytkin on oppinut porttikytköksen. Kuten portin perusteella valitussa reitityksessä myös tässä tapauksessa liikennöinti jakaantuu tasaisesti eri verkkoadaptereille, mikäli virtuaalisten verkkoadapterien määrä on suurempi kuin fyysisten. Virtuaalisen lähdeportin perusteella ja MAC-osoitteen tiivisteen perusteella tehdyt reitit ovatkin hyvin samankaltaisia ja lopputulos kuorman tasapainottamisen kannalta on hyvin samankaltainen. Pieni ero on kuitenkin siinä, että MAC-osoitteen tiivisteen laskemiseen perustuva reititys kuormittaa ESXi-isäntäpalvelinta hieman enemmän kuin virtuaaliseen lähdeporttiin perustuva reititys. [18, s. 8]

Kuorman tasapainotuksen kolmannessa vaihtoehdossa ylälinkki valitaan jokaisen IP-paketin kohdalla sen lähde- ja kohdeosoitteista lasketun tiivisteen mukaan (route based on IP-hash). Mikäli kyseessä ei ole IP-paketti, lasketaan tiiviste niistä arvoista, jotka ovat lähde- ja kohdeosoitteiden kohdalla vaikka ne eivät sisältäisikään järkeviä osoitteita. IP-tiivisteeseen perustuvassa reitityksessä liikenteen jakautuminen fyysisille verkkoadaptereille riippuu TCP/IP-istuntojen määrästä yksittäisiin kohdeosoitteisiin. Tämä tarkoittaa siis sitä, että IP-tiivisteeseen perustuvassa reitityksessä hyötyä ei saada suurien datamäärien siirrossa kahden yksittäisen isännän välillä. Yksi ratkaisu tähän on käyttää linkkien aggregointia (link aggregation). Tällä tarkoitetaan useiden fyysisten verkkoadaptereiden linkittämistä yhteen, jotta saadaan muodostettua nopea siirtoväylä yhdelle virtuaaliselle verkkoadapterille virtuaalisessa tietokoneessa. Linkkien aggregointia käytettäessä datapakettien heijastumiset estetään, sillä aggregoidut portit eivät uudelleenlähetä yleislähetys- tai ryhmälähetysliikennettä. Lisäksi fyysinen kytkin näkee porttikytköksissään virtuaalisen verkkoadapterin MAC-osoitteen useassa eri portissa, joten on mahdotonta ennustaa minkä portin kautta saapuva liikenne kuljetetaan, sillä se voi kulkea minkä tahansa portin kautta. [18, s. 8]

Neljäntenä tapana kuorman tasapainottamiseen on kuormaan perustuva reitinvalinta (Load Based Teaming) ja se toimii vain dvSwitchissä, josta kerrotaan tarkemmin kappaleessa ”dvSwitch”. LBT:n avulla reitti valitaan perustuen fyysisen verkkoadapterin kuormitukseen. Käytännössä tämä toimii niin, että ESXi-isäntäpalvelin tarkistaa tasaisin väliajoin jokaisen ryhmitykseen kuuluvan fyysisen verkkoadapterin kuormituksen ja tasapainottaa tämän jälkeen kuormat niiden mukaan. Mikäli yksi verkkoadaptereista on ylikuormitettu, se määrittelee uuden reitin liikenteelle, kunnes kuormat ovat jaettu tasaisesti käytössä olevien fyysisten verkkoadaptereiden kesken. LBT mahdollistaa dynaamisen kuorman tasapainottamisen säätämisen ja lisäksi se ottaa huomioon erilaisten fyysisten verkkoadapterien suorituskyvyn. Tämä mahdollistaa siis esimerkiksi 1 Gb, 10 Gb ja jopa 100 Mbit verkkoadaptereiden käytön ja samassa toteutuksessa ja silti kuorma pysyy jaettuna tasaisesti näiden välillä. LBT:ssä on otettava kuitenkin huomioon, että suurin mahdollinen kaistanleveys, joka voidaan saavuttaa, on yksittäisestä fyysisestä verkkoadapterista riippuva eli LBT ei yhdistä useiden verkkoadaptereiden nope-

uksia yhdeksi suuremmaksi. Lisäksi on huomioitava, että käytettävän fyysisen verkkoadapterin vaihtuessa toiseen fyysiseen verkkoadapteriin, liikenne alkaa kulkea fyysisessä kytkimessä eri portista kuin aikaisemmin, joten samasta MAC-osoitteesta tulleen liikenteen siirtyminen toiseen porttiin tulee olla sallittua fyysisen kytkimen osalta. [22]

Fyysisten verkkoadaptereiden ryhmityksessä on huomioitava seuraavat asiat: kaikkien fyysisten verkkoadaptereiden, jotka kuuluvat ryhmitykseen, pitää olla kytkettyinä samaan fyysiseen kytkimeen tai sopivaan fyysisten kytkinten pinoon. Fyysisessä kytkimessä tai useampien fyysisten kytkinten pinossa on oltava 802.3ad-tuki ja niiden tulee olla konfiguroitu käyttämään linkkien aggregointia staattisessa tilassa eli ilman LACP-ominaisuutta. Lisäksi kaikkien verkkoadapterien tulee olla aktiivisena. [18, s. 8]

Kuorman tasapainottamisella yleisesti saavutetaan tasaisempi verkon resurssien käyttö ja näin myös hyödytään kaikista avoinna olevista liikennöintiresursseista. Tasapainottamisen reititystavaksi on syytä valita parhaiten omaan pilvipalveluun sopiva määrittely.

Failover-konfiguraatiot

Failoverilla tarkoitetaan tilannetta, jossa liikenne ohjataan kulkemaan varalla olevan siirtotien kautta kun ensisijaiseen siirtotiehen tulee vikatilanne. Failover-konfiguraatiot ovat erilaisia tapoja havaita vikatilanne. Failover on suunniteltu nimenomaan varmistamaan fyysisen verkkoadapterin kautta kulkevan liikenteen sujuva toiminta. Failover konfiguraatioita on kaksi: Link Status only ja Beacon Probing.

Link Status only -asetuksessa vikatilanne havaitaan nimenomaisesti vain fyysisen verkkoadapterin vikatiloista, jotka itse fyysinen verkkoadapteri havaitsee. Näihin vikoihin kuuluvat esimerkiksi kaapelien irrotus fyysisestä verkkoadapterista tai verkkoadapteriin kytketyn fyysisen kytkimen vikatila. Link Status only -asetus ei kuitenkaan tunnista verkkokonfiguraatioon liittyviä vikoja, kuten tilannetta jossa spanning tree -protokolla estää fyysisen kytkimen portin toiminnan, asetuksiin on laitettu väärä VLAN eikä myöskään kaapelin irrotusta fyysisen kytkimen ylälinkin puolella.

Beacon Probing voidaan ajatella tukena Link Status only -asetukselle. Beacon Probing lähettää testikehyksiä ulospäin verkosta kaikille lähimmille verkkolaitteille ja odottaa niihin vastausta, havaiten näin tarkemmin vikatilanteita verkossa. Beacon Probing käyttää hyväkseen myös Link Status only -asetuksen saamia tietoja ja yhdistämällä ne omiin verkon toiminnan testauksiin saa se jo luotettavammin havaittua verkon vikatilanteita. Beacon Probing on hyödyllisin selvittämään ESXi-isäntäpalvelinta lähinnä olevan fyysisen kytkimen vikatilanteita, joissa Link Status only -asetus ei vielä havaitse vikatilannetta.

Fyysisten verkkoadaptereiden ryhmityksessä on oletuksena käytössä failback-sääntö. Tämä tarkoittaa sitä, että jos jokin fyysinen verkkoadapteri on joutunut vikatilaan ja liikenne on siirtynyt vaihtoehtoiselle reitille, palautuu se takaisin liikennöimään ensisijaisen verkkoadapterin kautta, jos se palautuu vikatilasta. Mikäli kyseessä on ajoittain toimiva fyysinen verkkoadapteri, saattaa tämä sääntö aiheuttaa turhaa edestakaista reitin vaihtumista, joten sääntö on mahdollista kytkeä pois päältä, jolloin liikenne kul-

kee varalla olevan siirtotien kautta kunnes se manuaalisesti palautetaan kulkemaan ensisijaisen verkkoadapterin kautta. Lisäksi tämä sääntö saattaa aiheuttaa sen, että fyysinen kytkin, johon verkkoadapterit on kytketty, ei salli liikennettä välittömästi tiettyyn porttiin, koska siihen kytketyn verkkoadapterin MAC-osoite vaihtuu liian usein. Jotta viiveet tässä tapauksessa saadaan mahdollisimman pieneksi, tulee käytössä olevasta fyysisestä kytkimestä kytkeä Spanning tree -protokolla, PAgP tai LACP sekä trunking negotiation pois käytöstä. Näiden avulla säästetään aikaa jopa yli 30 sekuntia vikatilanteen sattuessa. Toinen vaihtoehto viiveen minimoimiseksi on kytkeä aikaisemmin mainittu failback-sääntö pois päältä, jolloin ensisijainen adapteri jätetään varaväyläksi, vaikka se palautuisikin vikatilanteesta. VMware on lisännyt vielä yhden ominaisuuden viiveiden pienentämiseksi vikatilanteissa. Notify Switches -säännön avulla määritetään kommunikoiko ESXi-isäntäpalvelin fyysisen kytkimen kanssa vikatilanteen sattuessa. Mikäli sääntö on käytössä, ESXi-isäntäpalvelin lähettää vikatilanteessa fyysiselle kytkimelle kehotuksen päivittää osoitetaulunsa. Tämä johtuu tietenkin siitä, että MAC-osoite verkkoadapterissa vaihtuu ja liikenne alkaa kulkea tätä kautta. Tällöin fyysinen kytkin tunnistaa muutoksen nopeammin ja liikenteeseen ei tule niin suurta katkosta.

Failover Order -asetusten avulla voidaan määrittää miten kuorma tasapainotetaan. Osa fyysisistä verkkoadaptereista voidaan määrittää aktiivisiksi, osa jättää valmiustilaan varayhteyttä varten ja osa jättää kokonaan pois fyysisten verkkoadapterien ryhmityksestä.

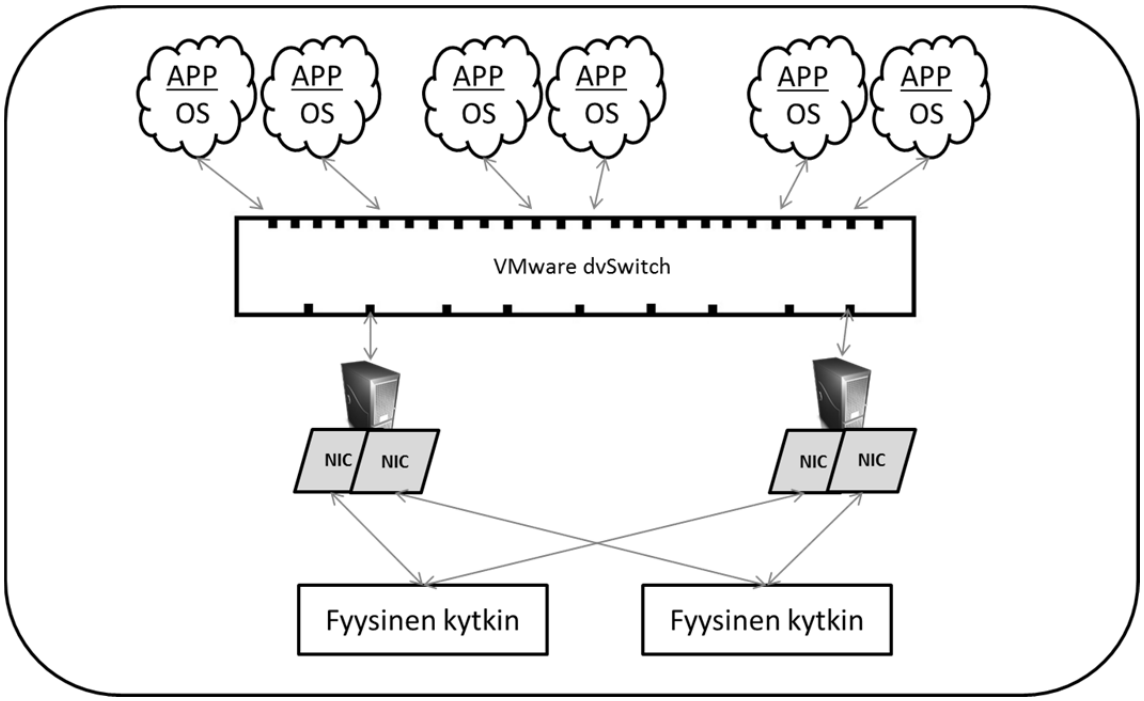
Fyysisten verkkoadaptereiden ryhmityksen avulla voidaan fyysisestä verkon osuudesta tehdä toimintavarma tai ainakin nopeasti toimintaan palautuva järjestelmä. Lisäksi kuorman tasapainottaminen eri reititystapojen avulla auttaa pilvipalveluinfrastruktuuria toimimaan juuri niin kuin sen pitääkin, käyttäen kaikki resurssit mahdollisimman tehokkaasti hyväksi. [18, s. 9]

Virtuaalisen kytkimen siirtoyhteyskerroksen tietoturva

Virtuaalisen kytkimen on mahdollista tehostaa tietoturvaa entisestään. Nämä tietoturvaominaisuudet koostuvat kolmesta eri ominaisuudesta. Promiscuous mode on asetus, joka sallii yksittäisten virtuaalisten tietokoneiden nähdä oman liikenteensä lisäksi muidenkin verkossa olevien laitteiden täsmälähetettyä liikennettä ja tämän vuoksi promiscuous mode -asetus on oletuksena kytketty pois päältä. MAC-osoitteen muuttamiskielto estää virtuaalisia tietokoneita vaihtamasta omaa yksittäislähetysosoitettaan. Tämä kielto estää myös muiden virtuaalisten tietokoneiden verkkoliikenteen näkemisen. Kolmantena forged transmit blocking -asetus estää virtuaalisia tietokoneita lähettämästä liikennettä, joka vaikuttaisi tulevan joltain muulta lähettäjältä kuin itse kyseessä olevalta tietokoneelta. Nämä kolme ominaisuutta varmistavat siis pääasiassa sen, että lähettäjä on juuri se jonka kytkin tietääkin sen olevan. Esimerkiksi jos pilvipalveluntarjoaja vuokraa yksittäisiä palvelimia asiakkailleen, on hyvin tärkeää, että pystytään varmistamaan asiakkaiden erottelu toisistaan ja estämään myös väärinkäyttötilanteita. [18, s. 31]

4.1.3 VMware dvSwitch - hajautettu virtuaalinen kytkin

Luvussa 4.1.2 esiteltiin tavallinen virtuaalinen kytkin eli vSwitch, sen komponentit ja toiminta. VMware on tavallisen virtuaalisen kytkimen lisäksi kehittänyt myös hajautetun virtuaalisen kytkimen, joka on tavallaan paranneltu versio tavallisesta kytkimestä. Hajautettu virtuaalinen kytkin, jota kutsutaan dvSwitch nimellä sisältää useita lisäominaisuuksia ja mahdollistaa aiempaa laajempien verkkojen luomisen. Periaatteessa hajautetun virtuaalisen kytkimen idea on päästä eroon useista yksittäisistä tavallisista virtuaalisista kytkimistä ja luoda niiden tilalle yksi hajautettu virtuaalinen kytkin jota pystytään hallitsemaan ja valvomaan hallintaohjelmistoilla datakeskuksen tasolla. Tavallinen virtuaalinen kytkin konfiguroidaan siis aina yksittäiseen ESXi-isäntäpalvelimeen, kun taas hajautettu virtuaalinen kytkin voidaan konfiguroida esimerkiksi kolmen ESXi-isäntäpalvelimen yhteiseksi kytkimeksi. Kuvassa (Kuva 6) esimerkki dvSwitchin toiminnasta, jossa fyysinen verkkoliikenne on lisäksi kahdennettu kahden ESXi-isäntäpalvelimen välillä.[23]



Kuva 6: Kahden isäntäkoneen yhteinen dvSwitch, jossa fyysinen verkkoliikenne on lisäksi kahdennettu.

Hajautettu virtuaalinen kytkin sisältää samat peruskomponentit kuin tavallinen kytkin kuten virtuaaliset portit, ylälinkki-portit ja porttiryhmät, ne ovat vain nimetty hieman eri tavalla. Esimerkiksi porttiryhmät ovat hajautettuja porttiryhmiä ja virtuaaliset portit ovat hajautettuja virtuaalisia portteja. Molemmat virtuaalisen kytkimen versiot sisältävät seuraavat toiminnallisuudet: kyky lähettää siirtoyhteyskerroksen kehyksiä eteenpäin, liikenteen jakaminen VLANeihin, VLAN-merkinnän (802.1q) ymmärtäminen, fyysisten verkkoadaptereiden ryhmittäminen ja uloslähtevän verkkoliikenteen

muokkaaminen. Hajautettuun virtuaalisen kytkimeen on lisätty vielä seuraavat ominaisuudet: saapuvan verkkoliikenteen muokkaaminen, keskitetty hallinta vCenterin avulla sekä tuki yksityisille VLANeille (Private VLAN). [24]

Verkkoliikenteen muokkaaminen

Tavallisella virtuaalisella kytkimellä voidaan siis muokata virtuaalisesta tietokoneesta ulospäin lähtevää liikennettä eli virtuaaliselta tietokoneelta vSwitchille saapuvaa liikennettä VNIC-kohtaisesti, mutta hajautetulla kytkimellä voidaan muokata myös virtuaaliselta kytkimeltä virtuaaliselle tietokoneelle saapuvaa liikennettä. Tämä on dvSwitchin lisätty lisäominaisuus. Käytännössä verkkoliikenteen muokkaaminen on melko yksinkertainen toimenpide virtuaalisessa ympäristössä. Hajautetun virtuaalisen kytkimen tapauksessa sen asetuksista voidaan muokata liikenteen muokkaus erikseen kumpaan suuntaan tahansa. Oletuksena verkkoliikenteen muokkaus on pois päältä. Verkkoliikennettä voidaan muokata kolmella eri tavalla: keskimääräisen kaistanleveyden mukaan (average bandwidth), kaistanleveyden maksimiarvon mukaan (peak bandwidth) tai purskeen koon mukaan (burst size). Käytännössä etuna sisäänpäin tulevan verkkoliikenteen muokkaamiselle on se, että virtuaaliselta tietokoneelta hajautetulle kytkimelle tulevaa verkkoliikennettä voidaan rajoittaa haluttaessa. Tämä saattaa tulla tarpeelliseksi esimerkiksi, kun halutaan rajoittaa tietyn pilvipalveluasiakkaan palvelinten verkkokapasiteetin käyttöä pilviympäristössä. Saapuvalla liikenteellä tarkoitetaan tässä tapauksessa siis virtuaaliselta tietokoneelta virtuaaliselle kytkimelle tulevaa liikennettä ja lähtevällä liikenteellä virtuaaliselta kytkimeltä virtuaaliselle tietokoneelle lähtevää liikennettä. [25]

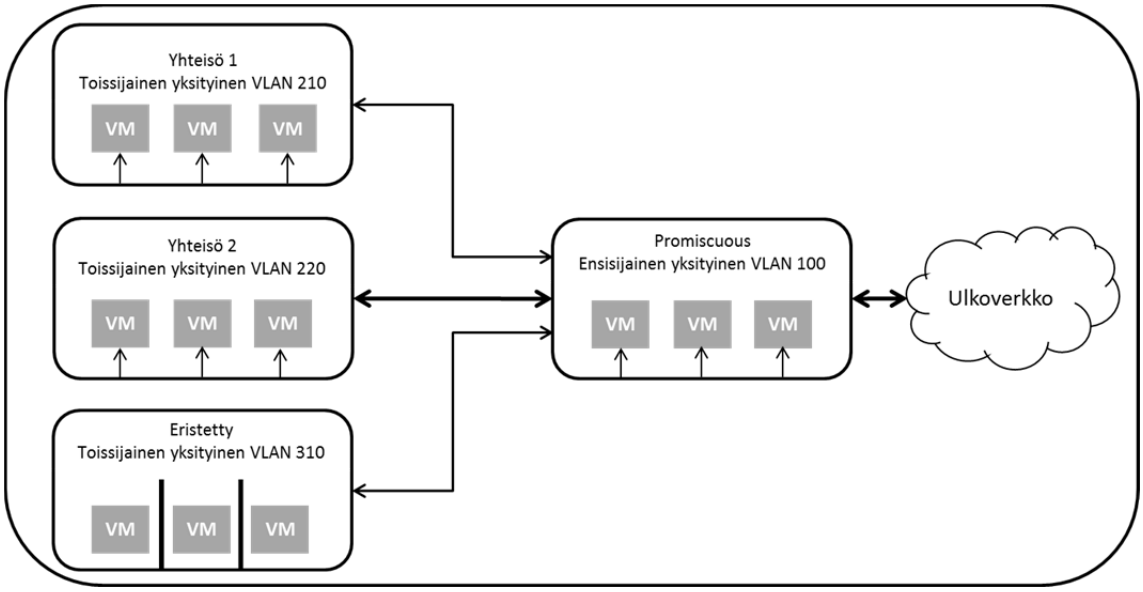
Keskitetty hallinta

Keskitetty hallinta ei sinällään kerro asiasta sen tarkemmin. Sillä tarkoitetaan eroa tavalliseen virtuaaliseen kytkimeen, joka on hallittavissa yhden ESXi-isäntäpalvelimen kautta. Keskitetyn hallinnan avulla voidaan useiden eri ESXi-isäntäpalvelinten yhteistä hajautettua virtuaalista kytkintä hallita yhden hallintaohjelmiston, vCenter Serverin kautta, mikä yksinkertaistaa hallintaa. Lisäksi keskitetty hallinta vähentää konfiguraatiovirheitä ja varmistaa HA:n (High Availability) toimivuuden. Parhaiten keskitetyn hallinnan ja samalla hajautetun virtuaalisen kytkimen toiminnan ymmärtää kuvasta (Kuva 6). Kuvasta selviää, että dvSwitchin tapauksessa hallinta koko klusterin hallinta onnistuu yhden vCenter Serverin avulla.

Yksityiset VLANit

Yksityiset VLANit eli PVLANit (Private VLAN) ovat ratkaisu kahteen ongelmaan. Niiden avulla päästään osittain eroon VLANien rajoitetusta määrästä sekä estetään IP-osoitteiden turha käyttö tietyissä verkkokonfiguraatioissa. Yksityiset VLANit jaetaan kahteen eri tyyppiin: ensisijainen yksityinen VLAN ja toissijainen yksityinen VLAN. Yksityinen VLAN määritellään ensisijaisen yksityisen VLAN-numeron avulla. Ensisijaisella yksityisellä voi taas olla useita toissijaisia yksityisiä VLANeja. Näin ollen voi-

daan ajatella ensisijaisen VLANin olevan portti useisiin toissijaisiin VLANeihin. Ensisijainen yksityinen VLAN toimii promiscuous-moodissa, millä tarkoitetaan sitä että se pystyy keskustelemaan muiden porttien kanssa, jotka ovat määritelty ensisijaisiksi VLANeiksi. Ensisijainen VLAN kannattaa ajatella reitittimeksi ulkoverkon ja toissijaisten VLANien välillä. Toissijaiset VLANit voivat toimia vielä lisäksi kahdessa eri moodissa: eristetyssä moodissa (isolated) tai yhteisö-moodissa (community). Eristetyssä moodissa olevat toissijaisen VLANin portit voivat keskustella ainoastaan promiscuous-moodissa olevien porttien kanssa ja yhteisö-moodissa olevat toissijaisen VLANin portit voivat taas keskustella joko samassa moodissa niiden kanssa olevien porttien tai promiscuous-moodissa olevien porttien kanssa. On huomioitavaa, että eristetyssä moodissa olevat eivät voi keskustella edes samassa moodissa olevien porttien kanssa vaan ainoastaan promiscuous-moodissa olevien kanssa. Lisäksi eristetyssä moodissa oleva toissijainen VLAN on uniikki, eli niitä voi olla vain yksi kappale yksityistä VLANia kohden. Kuvassa (Kuva 8) on esitetty yksityisten VLANien käyttöä. [26 ; 27]



Kuva 7: Yksityisen VLANin käyttö ja eri moodit. [27]

Yksityisiä VLANeja voidaan käyttää jakamaan verkkoa useampiin osiin jolloin kaikki yksityiset toissijaiset VLANit voivat jakaa saman IP-aliverkon. Yksityisiä VLANeja käytetään myös tapauksissa, joissa halutaan yhden palomuurin taakse jopa tuhansia liityntäpisteitä ja näin säästytään konfiguroimasta palomuuria erikseen jokaiselle VLANille. Jotkin palomuurit lisäksi vaativat lisenssimaksuja jokaista VLANia kohden, joten PVLANien avulla tästä päästään eroon. [28]

Edellä mainittujen eroavaisuuksien lisäksi uusimmissa dvSwitchien versioissa toiminnallisuutta on parannettu seuraavilla päivityksillä: toiminnalliset parannukset, verkon valvonnan ja vianrajauksen parannukset sekä skaalautuvuuden ja laajennettavuuden parantaminen.

Toiminnalliset parannukset

Toiminnallisten parannusten tarkoituksena on parantaa vSphere-pilviympäristön ylläpitäjiä hallitsemaan virtuaalista verkkoa tehokkaammin ja helpottaa ylläpitäjien työtä vialisten konfiguraatioiden tapauksessa. vSphere nimitystä käytetään koko VMwaren pilviympäristöstä ja se on kokonaisuus, joka sisältää kaikki pilviympäristön komponentit, kuten vCenter Serverin ja ESXi-isäntäpalvelimen. Alkuperäisen vSphere 4.0 -versiossa julkaistun dvSwitchin kanssa käyttäjillä on ollut ongelmia esimerkiksi koko datakeskusta koskevan vian jälkeisessä verkon palautumisessa ja silloin, kun he ovat menettäneet vCenter Serverin kautta olevan hallinnan konfiguraatiovirheiden vuoksi. Näiden tilanteiden vuoksi hajautettuun virtuaaliseen kytkimeen on vSphere 5.0 -versiossa lisätty seuraavat toiminnot: Network health check eli verkon tilan tarkistus, dvSwitchin konfiguraation varmistus ja palautus, hallintaverkon palautuspiste (rollback and recovery), hajautetun virtuaalisen portin automaattinen lisäys (Auto Expand), MAC-osoitteen hallinta, LACP-protokollan tuki sekä Bridge Protocol Data unit suodatus. Uusin vSphere-versio on 5.5 ja se sisältää luonnollisesti edellä mainitut toiminnalliset parannukset, jotka tehtiin versioon 5.0.

Network health check eli verkon tilan tarkistus on ominaisuus joka tunnistaa verkossa mahdollisesti olevat vialliset konfiguraatiot VLANin ja MTU:n osalta. Kun virtuaalinen verkko luodaan ja portteja provisioidaan tietyille virtuaalisille tietokoneille, tulee määrittää myös VLANit sekä MTU:t. Nämä konfiguraatiot tulee tehdä sekä virtuaalisiin kytkimiin kuin myös fyysisiin kytkimiin. Aikaisemmissa hajautetuissa virtuaalisissa kytkimissä tai tavallisissa virtuaalisissa kytkimissä näiden konfiguraatioiden oikeellisuutta ei tarkastettu millään tavalla. Network health check -ominaisuuden onkin tarkoitus tarkistaa säännöllisin aikavälein VLANin toimivuus, MTU-arvon virheettömyys sekä fyysisten adaptereiden ryhmitysten toimivuus. Aikaväli näille tarkistuksille on oletuksena yksi minuutti, jolloin hajautettu virtuaalinen kytkin lähettää verkkoon kyselyjä (REQ-packets) ja jää odottamaan vastauksia (ACK-packets). Mikäli hajautettu virtuaalinen kytkin ei saa takaisin vastauksia, se varoittaa mahdollisesta konfiguraatiovirheestä hallintaohjelmiston kautta. VLAN- ja MTU-tarkistukset vaativat toimiakseen vähintään kaksi fyysistä ylälinkkiä dvSwitchissä ja ryhmityksen tarkistus vaatii toimiakseen sen, että dvSwitchiin on kytketty vähintään kaksi ESXi-isäntäpalvelinta ja dvSwitchiin tehdyssä ryhmityksessä on vähintään kaksi aktiivista fyysistä ylälinkkiä. [29, s.3-4]

DvSwitchin konfiguraation varmistus ja palautus tekee varmuuskopion olemassa olevasta virtuaalisesta verkosta ja kytkimen konfiguraatioista, jotta se voidaan palauttaa vikatilanteen sattuessa. DvSwitchiä hallitaan vCenter Serverin kautta ja kaikki konfiguraatiotiedot tallennetaan sen tietokantaan. Näin ollen aikaisemmin ei ollut mahdollista varmuuskopioida tai palauttaa aikaisempaa konfiguraatiota vCenter Serverin tietokannan tiedostojen korruptoituessa tai muissa vikatapauksissa. Näissä tilanteissa virtuaalisen verkon joutui luomaan alusta asti uudestaan porttiryhmiä ja yksittäisiä konfiguraatioita myöden. Varmistus ja palautus -ominaisuuden avulla verkon konfiguraatioista voidaan ottaa täydellinen varmuuskopio, joka voidaan helposti palauttaa käyttöön. Var-

muuskopion ottaminen mahdollistaa myös sen, että verkon konfiguraatio voidaan helposti kopioida toiseen datakeskukseen. Varmuuskopiot voidaan ottaa joko paikalliselle levylle tai verkkolevylle hallintaohjelmiston kautta. Kun varmuuskopioita otetaan säännöllisesti, voidaan myös helposti palata edelliseen konfiguraatioon, mikäli todetaan muutosten aiheuttaneen ongelmia verkon toiminnassa, sillä varmistus ja palautus -ominaisuus tallentaa varmuuskopiot uusina versioina eikä vanhan varmuuskopion päälle. [29, s. 4]

Hallintaverkon palautus -toiminto on äärimmäisen tärkeä dvSwitchin kannalta. Kuten aikaisemmin on mainittu, tavallista virtuaalista kytkintä hallitaan ESXi-isäntäkohtaisesti ja hajautettua virtuaalista kytkintä keskitetyn hallinnan avulla. Keskitetty hallinta helpottaa asioita, mutta sen joutuessa vikatilaan ei aikaisemmin ollut mahdollista konfiguroida hajautettua kytkintä uudelleen. Tällöin jouduttiin mahdollisesti luomaan jokaiselle ESXi-isäntäpalvelimelle erikseen tavallinen virtuaalinen kytkin ja kun kaikki ESXi-isäntäpalvelimet oli konfiguroitu näin, pystyttiin keskitetyn hallinnan kautta luomaan uudelleen hajautettu virtuaalinen kytkin. Yksinkertaisesti sanottuna vikatilanteessa siis menetetään verkkoyhteys vCenter Serveriin, jolloin myöskään hallinta ei toimi. Hallintaverkon palautus -toiminto huomaa automaattisesti verkkoon tehdyt muutokset ja tekee yhteystestin vCenter Serveriin. Mikäli vCenter Serveriin ei enää saada yhteyttä verkkomuutoksen jälkeen, se palauttaa aikaisemmat konfiguraatiot ja verkon toiminta palautuu aikaisempaan, toimivaan konfiguraatioon. Tämän toiminnon lisäksi on hajautetun virtuaalisen kytkimen hallintaverkko mahdollista konfiguroida suoraan konsolin ESXi-isäntäpalvelinta käyttäen. [29, s. 5]

Hajautetun virtuaalisen portin automaattinen lisäys helpottaa porttien provisiointi virtuaalisille tietokoneille. Hajautettu virtuaalinen portti yhdistää virtuaalisen tietokoneen dvSwitchiin. Aikaisemmin oli mahdollista tehdä porttiliitoksia kytkimen ja tietokoneen välille kolmella eri tavalla: staattinen sidonta (static binding), dynaaminen sidonta (dynamic binding) ja hetkellinen sidonta (ephemeral binding). Staattisella sidonnalla tarkoitetaan sitä, että porttiryhmään annetaan tietty määrä portteja ja kun uusi virtuaalinen tietokone käynnistetään, portti yhdistetään tähän tietokoneeseen. Vaikka virtuaalinen tietokone sammutetaan, portti pysyy sidottuna tähän tietokoneeseen. Dynaaminen sidonta toimii muuten samalla tavalla kuin staattinen sidonta, mutta porttisidonnat eivät säily kun virtuaalinen tietokone sammutetaan. Dynaaminen sidonta on vanha tapa tehdä porttikytköksiä ja sitä ei ole enää saatavilla uusimmissa vSphere versioissa. Hetkellisessä sidonnassa ei tehdä minkäänlaista provisiointia porttien suhteen, joten se toimii vastaavalla tavalla kuin tavallinen virtuaalinen kytkin. Hajautettu porttiryhmä kytkee sille annettuun maksimäärään asti virtuaalisia tietokoneita sen portteihin aina kun niitä yhdistetään dvSwitchin porttiryhmään. Staattisen sidonnan etuna on se, että sen avulla tietyille porteille provisioidut virtuaaliset tietokoneet pysyvät aina samoissa porteissa ja näin ollen niiden tilaa voidaan seurata. Tämän vuoksi staattista sidontaa on hyvä käyttää, mikäli halutaan säilyttää tietyn virtuaalisen tietokoneen verkon tilan näkyvyys ja mahdollisuus vianrajaukseen. Hajautetun virtuaalisen portin automaattisen lisäyksen myötä staattisen sidontaan on tullut lisäominaisuus joka helpottaa porttiryhmien

konfigurointia. Aikaisemmin porttiryhmään kuuluvien porttien määrä piti määrittää konfigurointivaiheessa ja mikäli porttiryhmään kytkettiin tätä arvoa suurempi määrä virtuaalisia tietokoneita, portit loppuivat kesken. Automaattisen lisäyksen avulla porttiryhmä tunnistaa, että on tarve lisäporteille ja konfiguroi niitä automaattisesti lisää porttiryhmään. Tämän avulla porttiryhmien porttimääriä ei tarvitse tietää tarkalleen ennalta, mikä helpottaa verkon suunnittelua ja konfigurointia. [29, s. 5-6]

VSphere -pilviympäristössä vCenter Server allokoi MAC-osoitteet virtuaalisten tietokoneiden virtuaalisille verkkoadaptereille. MAC-osoitteiden tulee olla uniikkeja siirtoyhteyskerroksen yleislähetys-tasolla. Aikaisemmassa dvSwitchissä jokainen vCenter Server pystyi allokoimaan 64000 MAC-osoitetta. Tämä määrä ei kuitenkaan riitä, varsinkaan kun kyseessä on isot pilviympäristöt. Myös duplikaatti-MAC -osoitteiden mahdollisuus oli olemassa esimerkiksi eri pilvipalveluntarjoajien välillä. MAC-osoitteiden hallinnan avulla on tullut mahdolliseksi käyttää paikallisesti hallinnoituja MAC-osoitteita, mikä yksinkertaistaa niiden hallintaa sekä parantaa skaalautuvuutta. Käyttäjät voivat määrittää MAC-osoitteen prefiksit sekä MAC-osoitealueet itse. Tämä tarkoittaa myös sitä, että VMwaren organisaatiolle määrättyä prefiksiä ei ole pakollista käyttää, mutta se on kuitenkin edelleen mahdollista. Pakollisen VMwaren prefiksin poistuminen tarkoittaa sitä, että käyttäjille avautuu käyttöön koko 48-bittinen MAC-osoitealue ja näin ollen MAC-osoitteita tulee olemaan yli 281 biljoonaa. Näin suuri määrä poistaa myös mahdollisuuden duplikaatti-osoitteisiin varsinkin kun eri yritykset käyttävät omia prefiksejään tai osoitealuettaan. [29, s. 6]

LACP-protokollan tuki on myös lisätty vSphere 5.0 -versiosta alkaen. LACP-protokollaa ei edelleenkään tueta tavallisessa virtuaalisessa kytkimessä. LACP-protokolla on standardeihin perustuva tapa hallita useiden fyysisten linkkien yhdistämistä loogiseksi kanavaksi paremman kaistanleveyden ja redundanssin saavuttamiseksi. LACP-protokollan avulla verkkolaitteet voivat automaattisesti neuvotella yhdistämisestä lähettämällä LACP-paketteja. Aikaisempaan staattisen fyysisten verkkokorttien linkitystapaan verrattuna LACP-protokolla mahdollistaa plug and play -konfiguroinnin eli automaattisen keskustelun virtuaalisen isäntäkoneen ja fyysisen kytkimen välillä. LACP-protokolla myös tunnistaa automaattisesti ylälinkkien vikatilat ja virheelliset kytkennät kaapeloinnissa ja konfiguroi ylälinkit uudelleen. [29, s. 6]

Bridge Protocol Data Unit- eli BPDU-suodatin on sääntö spanning tree -protokollan aiheuttamille ongelmille. BPDU-paketit ovat osa STP-protokollaa ja niitä käytetään selvittämään verkon topologiaa. Kumpikaan virtuaalisista kytkimistä ei tue STP-protokollaa eikä näin ollen osallistu BPDU-pakettien lähettämiseen tai vastaanottamiseen. BPDU-paketit saattavat kuitenkin aiheuttaa ongelman siinä tapauksessa, että virtuaalinen tietokone lähettää niitä ja fyysinen kytkin havaitsee ne, sillä vaikka virtuaaliset kytkimet eivät näitä paketteja lähetä, ne kuitenkin ohjataan eteenpäin fyysiselle kytkimelle. Kun fyysisen kytkimen portti vastaanottaa BPDU-paketin ja porttiasetuksissa on BPDU-guard -asetus päällä, fyysisen kytkimen portti kytketään pois päältä vikatilan vuoksi. Näin tapahtuessa vSphere pilviympäristö huomaa viallisen fyysisen portin ja siirtää liikenteen kulkemaan toisen ylälinkin kautta, joka on kytketty fyysisen

kytkimen toiseen porttiin. Tällöin BPDU-paketit näkyvät myös fyysisen kytkimen toiselle portille ja kytkin sulkee tämänkin portin. Loppujen lopuksi tämä BPDU-pakettien lähetys aiheuttaa DOS-hyökkäyksen kaltaisen tilanteen koko virtuaalisen verkon kannalta. BPDU-suodattimen avulla voidaan suodattaa virtuaalisen tietokoneen lähettämät BPDU-paketit, ennen kuin ne pääsevät fyysiselle kytkimelle asti ja näin ollen estää tämänkaltaisten tilanteiden syntyminen. BPDU-suodatus lisää siis virtuaalisten kytkinten toimintavarmuutta entisestään ja estää DOS-hyökkäyksiä tehokkaasti. [29, s. 7]

Verkon valvonta ja vianrajaus

Verkon ylläpitäjien on usein tarve valvoa virtuaalisen infrastruktuurin verkkoliikennettä. Tätä varten VMware käyttää portin peilausta ja NetFlow ominaisuutta, joita on parannettu RSPAN (remote switched protocol analyzer) ja ERSPAN (encapsulated remote switched protocol analyzer) lisäominaisuuksilla. NetFlow tukee nyt versiota 10, joka on IETF:n standardisoima ja jota kutsutaan myös nimellä Internet Protocol Flow Information eXport (IPFIX). Lisäksi SNMP-protokolla tukee kaikkia kolmea protokollan versiota.

Portin peilauksella tarkoitetaan sitä, että käyttäjät voivat ottaa käyttöön RSPAN ja ERSPAN ominaisuudet kun halutaan keskitetysti valvoa verkkoliikennettä joko pakettikaappaajan tai verkkoanalysaattorin avulla, joka on useiden solmupisteiden takana valvotusta verkosta. Portin peilaus lähettää verkkoliikenteen kopioituna myös valvontapisteelle, jolloin kaikki haluttu verkkoliikenne nähdään myös valvontalaitteistolla. RSPAN vaatii toimiakseen oman VLANin, jonka avulla se kulkee useiden fyysisten kytkinten läpi haluttuun valvontapisteeseen. ERSPAN ominaisuus mahdollistaa verkkoliikenteen valvomisen IP-verkon takaa. Liikenne joka peilataan, lähetetään etäpisteessä toimivalle verkonvalvonnalle kapsuloidussa muodossa, jota kutsutaan myös nimellä GRE-tunneli. GRE on Ciscon kehittämä IP-tunnelointiprotokolla, jonka sisällä voidaan tunneloida esimerkiksi VPN-yhteyksiä ja tavallisia IP-paketteja. ERSPAN on siis reititettävä versio RSPANista. [29, s. 7-8]

IPFIX on kehittynyt ja joustava protokolla, jonka avulla käyttäjät voivat määrittää NetFlow-tallenteet, jotka kerätään dvSwitchillä ja lähetetään kerääjätyökalulle. IPFIXiä voidaan käyttää esimerkiksi tilanteessa, joissa halutaan selvittää tietystä IP-osoitteesta toiseen tiettyyn IP-osoitteeseen kulkevien IP-pakettien lukumäärä ja näin havainnollistaa kuinka suuresta liikennemäärästä on kyse. Reitittimien tapauksessa liikennemäärästä voidaan päätellä kuinka suuri verkko reitittimen takana on. IPFIXillä voidaan valvoa esimerkiksi IPv6-, MPLS- ja VXLAN-liikennettä. [29, s. 9]

ESXi-isäntäpalvelimet tukevat SNMP-agentin käyttöä. SNMP on standardisoitu protokolla, jonka avulla valvontalaitteistot voivat lähettää kyselyitä SNMP-agenteille ja saada näin niistä lisätietoa. Sen avulla voidaan lähettää kysely esimerkiksi verkkolaitteen tilasta tai laite voi itsenäisesti lähettää hälytyksiä valvontalaitteistolle. Parannetun SNMP-tuen avulla virtuaalista verkkoa ja sen tilaa voidaan valvoa entistä tarkemmin ja helpottaa vianrajausta. Yhdessä portin peilauksen ja IPFIXin kanssa dvSwitch tarjoaa ylläpidolle tehokkaat työkalut verkon tehokkaaseen ylläpitämiseen. [29, s. 9-10]

Muihin verkonvalvonnan ja vianrajauksen ominaisuuksiin kuuluvat vielä Netdump sekä SR-IOV (Single Root I/O Virtualization). Netdump on ominaisuus, jonka avulla VMkernelin core dumpit voidaan ohjata määrätylle verkon palvelimelle. Se käyttää UDP-protokollaa dump-tiedostojen siirrossa ja toimii asiakas-palvelin -periaatteella. Netdump tukee myös VLANien käyttöä. SR-IOV on standardi, joka mahdollistaa yhden PCI Express (PCIe) adapterin esittämisen loogisesti useana eri adapterina virtuaalisille tietokoneille. SR-IOV:n avulla voidaan esimerkiksi pienentää vasteaikaa ja vähentää prosessorin käyttöä. ESXi-alustoissa on myös VMwaren VMDirectPath läpäisyominaisuus, jonka avulla saavutetaan samoja hyötyjä. Sen käyttö vaatii kuitenkin sen, että jokaista virtuaalista tietokonetta kohden on yksi fyysinen verkkoadapteri. SR-IOV:n avulla voidaan samat hyödyt saavuttaa yhden fyysisen verkkoadapterin avulla. [29, s. 10]

Skaalautuvuuden parannukset

DvSwitchin skaalautuvuusmahdollisuudet ovat hyvät. Aikaisempia rajoituksia on nostettu uusimpaan vSphere 5.5-versioon merkittävästi. Yhtä vCenter Serveriä kohden voi olla yhteensä 128 dvSwitchiä. Vertailun vuoksi esimerkiksi aiemmassa 5.0-versiossa dvSwitchejä voitiin luoda 32 vCenteriä kohden. Lisäksi yhtä vCenter Serveriä kohden on mahdollista luoda 10000 staattista tai dynaamista porttiryhmää sekä yhteensä 60000 hajautettua virtuaalista porttia. Myös ESXi-isäntälaitteita voi olla yhtä dvSwitchiä kohden 1000 kappaletta. On tärkeää huomioida, että dvSwitchin idea on yhdistää useita eri ESXi-isäntälaitteita toisiinsa, joten skaalautuvuus on yksi tärkeimmistä dvSwitchin ominaisuuksista. [29, s. 32]

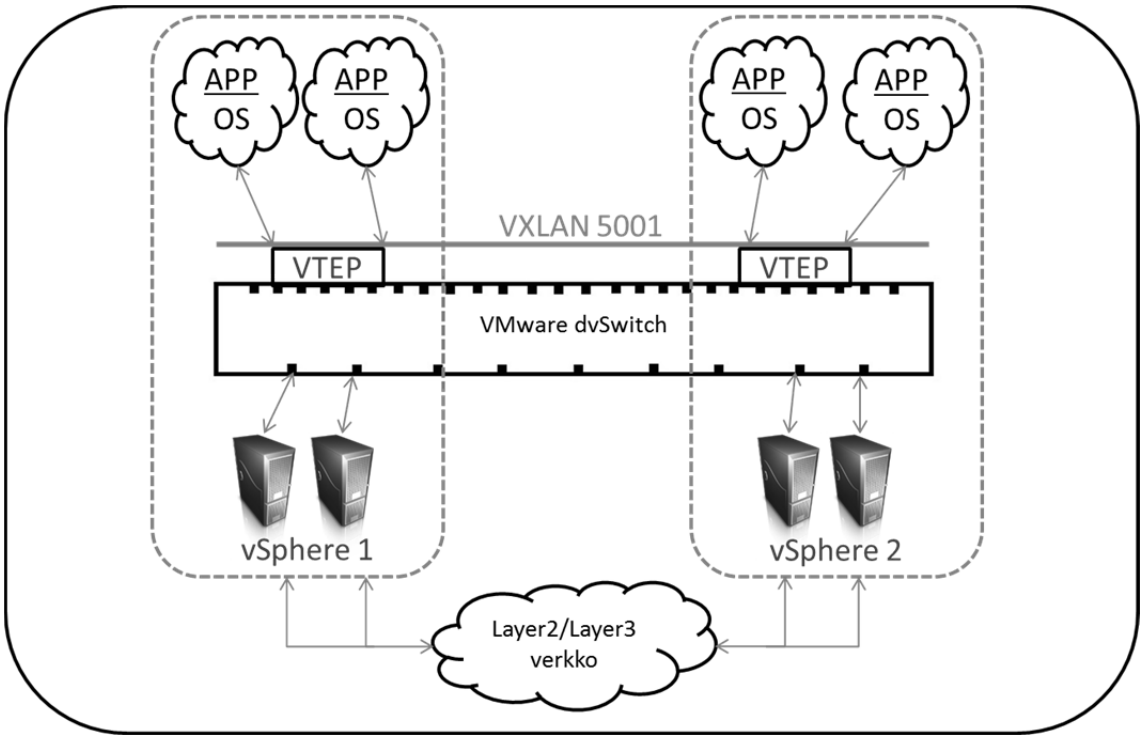
vSwitch vai dvSwitch?

Tämä kysymys ei ole niin yksiselitteinen kuin moni voisi ajatella. DvSwitch sisältää skaalautuvuudeltaan tehokkaampia ratkaisuja ja sen avulla koko pilviympäristöä ja sen virtuaalista verkkoa pystytään hallitsemaan yhdestä paikasta. Tämä saattaa kuitenkin olla ongelma jos vCenter Serveriin ei enää saada yhteyttä johtuen esimerkiksi konfiguraatiovirheestä. Toki dvSwitchiin on uusien vSphere-versioiden myötä päivitetty juuri tämänkaltaisten ongelmien takia uusia ominaisuuksia, joiden avulla verkon ja koko ympäristön toimivuus ja käyttöaste pystytään pitämään mahdollisimman korkealla, mutta näiden käyttö vaatii enemmän konfigurointia ja yleensäkin luottamuksen näiden ominaisuuksien varmaan toimimiseen. Useat pilviympäristön ylläpitäjät käyttävätkin hybridi-mallia. Hybridi-mallilla tarkoitetaan tässä tapauksessa, että käytössä on molempia virtuaalisia kytkimiä. Tämä lisää tietenkin pilviympäristön monimutkaisuutta, mutta sen avulla voidaan myös varmistaa toimivuutta. DvSwitchin ja vSwitchin hankintaa miettiessä kannattaa ottaa huomioon myös niiden kustannukset. VSwitch kuuluu halvimpaan VMwaren lisenssiin, mutta dvSwitchin käyttö vaatii kalleimman Enterprise Plus -lisenssin ostamisen, joten dvSwitchin käyttö on huomattavasti kalliimpaa. VMwaren työntekijä Duncan Epping on myös miettinyt vastausta tähän kysymykseen blogissaan ja päätynyt tulokseen, että valinta riippuu siitä mitä käyttäjä haluaa. Hybridi-mallilla ja

pelkillä dvSwitchien käytöllä on omat puolensa, mutta yleisesti ottaen dvSwitch mahdollistaa tehokkaamman ja helpomman virtuaalisen verkon luomisen. [30]

4.1.4 VXLAN

VXLAN (Virtual Extensible Local Area Network) on VMwaren, Ciscon ja Arista Networksin kehittämä teknologia, jonka avulla on mahdollista yhdistää kaksi eri siirtoyhteyskerroksen verkkoa eli lähiverkkoa toisiinsa kapsuloimalla siirtoyhteyskerroksen kehykset IP-paketiksi ja lähettämällä ne välissä olevan IP-verkon yli [31]. VXLAN käyttää kapsuloinnissa VLANin tyylistä kapsulointia ja se muodostaa kahden lähiverkon välille tunnelin, jossa tieto kuljetetaan. VXLANia kutsutaan myös overlay-teknologiaksi juuri siksi, että sen avulla voidaan OSI-mallin alemman kerroksen tietoa kuljettaa OSI-mallin ylemmän kerroksen avulla. Seuraavassa kuvassa (Kuva 9) on esitetty VXLANin looginen toiminta kahden pilviympäristön välillä. Periaatteessa VXLAN siis venyttää dvSwitchin kahden eri pilviympäristön välille vaikka käytännössä molemmissa ympäristöissä on käytössä omat dvSwitchit.

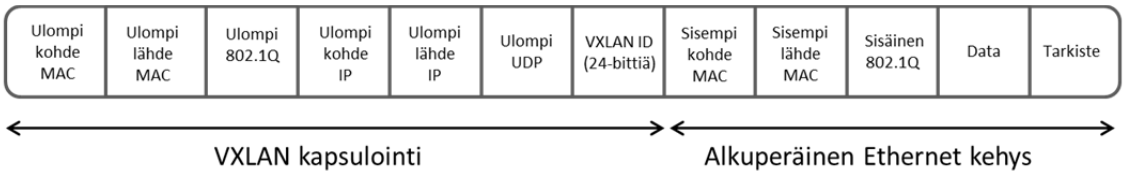


Kuva 8: VXLAN kokonaiskuva, jossa kaksi eri pilviympäristöä yhdistetty toisiinsa.

VXLAN kapsulointi

Kapsulointi tapahtuu VXLANissa niin, että MAC-kehys kapsuloidaan UDP-pakettiin. Kommunikointi kahden lähiverkon välillä tapahtuu muodostamalla VTEPien (Virtual Tunnel Endpoint) avulla tunneli niiden välille (Kuva 9). VTEPien tehtävä on kapsuloida MAC-kehykset ja vastaavasti toisessa päässä purkaa kapsulointi sekä ohjata paketit oikealle virtuaaliselle kohdetietokoneelle samanlaisena siirtoyhteyskerroksen kehyksenä, kuin se alun perin lähettiin. Seuraavassa kuvassa (Kuva 10) on esitelty VXLAN-

kapsuloitu otsake. Alkuperäiseen Ethernet-kehykseen lisätään 24-bittinen VXLAN-ID, ulompi UDP-otsake, ulompi lähteen IP-osoite, ulompi kohteen IP-osoite, ulompi 802.1Q- eli VLAN-tieto, ulompi lähteen MAC-osoite ja ulompi kohteen MAC-osoite. VXLAN-ID kenttä sisältää VXLAN-segmentin numeron. Ulompi UDP-otsake sisältää lähteen eli VTEPin UDP-portin ja kohteen UDP-portin. On suositeltavaa, että lähdeportti lasketaan tiivisteenä sisemmän Ethernet-kehyksen otsakkeesta. UDP-tarkistesumman tulee olla asetettu arvoon 0, sillä se pakottaa vastaanottajan purkamaan paketin kapsuloinnin, muussa tapauksessa saattaa vastaanottava VTEP päättää olla purkamatta kapsulointia ja hylätä sen. Tämä aiheuttaa siis periaatteessa tarpeettoman tarkisteen laskemisen vastaanottavassa päässä. Ulompaan lähde IP-osoitteen kenttään tulee sisemmän lähde MAC-osoitteen omaavan VTEPin IP-osoite ja vastaavasti ulompaan kohde IP-osoitteen kenttään tulee sisemmän kohde MAC-osoitteen omaavan VTEPin IP-osoite. Ulompi 802.1Q eli VLAN-merkintä kenttä on vapaavalintainen, joten sitä ei ole välttämätöntä käyttää. Ulompaan lähde MAC-osoitteen kenttään tulee joko lähde VTEPin MAC-osoite tai välissä olevan verkkokerroksen reitittimen MAC-osoite. Ulompi kohde MAC-osoite kenttä sisältää vastaavasti kohde VTEPin tai välissä olevan verkkokerroksen reitittimen MAC-osoitteen. [32, s. 10-11]



Kuva 9: VXLAN-kapsuloitu otsake. [33]

VXLAN mahdollistaa loogisen lähiverkon muodostamisen IP-verkon päälle. Jos kaksi lähiverkkoa halutaan yhdistää perinteisellä tavalla, niiden väliin tulee konfiguroida reititin tai useampia reitittimiä, jotta kahden lähiverkon välissä oleva kuilu saadaan yhdistettyä. VXLANin kanssa käytettävä vShield Edge mahdollistaa kahden eri VXLAN-segmentin kommunikoinnin keskenään. vShieldistä Edgestä kerrotaan lisää kappaleessa 3.3.7.

VXLAN vaatii toimiakseen seuraavat avainkomponentit: VMware vCloud Network and Security Manager (vCNS) -verkon hallinnan, VMware vSphere Distributed Switchin (dvSwitch), VTEPin sekä vShield Edge Gatewayn. VCNS on verkon hallinta -komponentti keskitettyyn vCloud Network and Security hallintaohjelmistoon. Luvussa 4.1.3 esitelty dvSwitch on myös tarpeellinen, sillä tavallinen vSwitch ei tue VXLANia. DvSwitchit tulee olla käytössä siis molemmissa yhdistettävissä lähiverkoissa. On myös hyvä huomioida, että Open vSwitch tukee VXLAN-teknologiaa, joten dvSwitchin käyttö ei ole täysin pakollista.

VTEP on osa dvSwitchiä ja sitä käytetään nimenomaan kapsuloinnissa ja sen purkamisessa. VTEP huolehtii reitin prosessoinnista, johon kuuluu kapsuloinnin lisäksi osoitetaulujen ylläpito. VXLAN-liikennettä välitetään pisteestä toiseen virtuaalisten

verkkoadaptereiden avulla. VTEPiin kuuluu vielä lisäksi VXLAN-porttiryhmät. VXLAN-porttiryhmien avulla määritetään fyysiset verkkoadapterit, VXLAN- tiedot ja ryhmityssäännöt. Nämä porttiryhmät määräävät miten VXLAN-liikenne kuljetetaan sisään ja ulospäin ESXi-isäntäpalvelimen VTEPien ja fyysisten verkkoadaptereiden läpi.

VShield Edge on virtuaalinen lisäohjelmisto, joka antaa virtuaaliselle verkolle perinteisiä vastaavia toiminnallisuuksia kuten palomuurin, DHCP:n ja NATin sekä VXLANin kannalta tärkeän VXLAN-yhdyskäytävä -toiminnon. VXLANin kannalta vShield Edge toimii läpinäkyvänä siltana VXLAN-infrastruktuurin ja tavallisen verkko-infrastruktuurin välillä. Kun VXLANiin kuuluva virtuaalinen tietokone haluaa kommunikoida fyysisen palvelimen kanssa tai virtuaalisen tietokoneen kanssa, joka ei kuulu VXLANiin, liikenne ohjataan kulkemaan vShield Edgen kautta. Kun VXLANissa oleva virtuaalinen tietokone haluaa kommunikoida toisen VXLANissa olevan virtuaalisen tietokoneen kanssa, niin vShield Edge tarjoaa myös tässä tapauksessa näiden pisteiden yhteyden. [33]

VXLANin hyödyt

VXLANin avulla voidaan yhdistää fyysisesti erillisiä pilviympäristöjä toisiinsa ja muodostaa näin keskitetysti hallittavia kokonaisuuksia. VXLAN auttaa siis siirtymisessä ohjelmallisesti hallittavaan datakeskus-malliin. Tämä helpottaa verkon hallintaa huomattavasti, sillä virtualisoitu verkko voidaan ohjelmoida yhdestä pisteestä. VXLANia käytettäessä eri aliverkoissa olevat virtuaaliset tietokoneet voivat keskustella toistensa kanssa ilman, että niiden välille tarvitsee konfiguroida fyysisiä kytkimiä tai reitittimiä eli se käyttää olemassa olevaa fyysistä siirtotietä hyväkseen. VXLAN toimii tavallisten kytkinten kanssa, jolloin verkkoa voidaan laajentaa käyttämällä vanhaa fyysistä verkko-infrastruktuuria eikä tarvetta ole myöskään ohjelmistopäivityksille tai erikoiskytkimille. Tämä helpottaa osittain VXLANin käyttöönottoa ja laskee investointikustannuksia. VXLAN mahdollistaa lisäksi hyvän skaalautuvuuden sillä sen avulla voidaan muodostaa yli 16 miljoona loogista verkkosegmenttiä. Skaalautuvuus on täten aivan eri luokkaa verrattaessa VXLANia tavalliseen VLANiin, jonka suurin mahdollinen loogisten verkkosegmenttien määrä on 4096. [33]

Huomioitavia asioita VXLANin käytössä

Kuten jo aikaisemmin mainittiin, VXLAN-teknologia toimii ainoastaan dvSwitchien kanssa. Lisäksi kannattaa huomioida seuraavat asiat. MTU-arvo tulee konfiguroida sekä ESXi-isäntäpalvelimissa kuin myös fyysisissä kytkimissä vähintään arvoon 1600. Tämä johtuu siitä, että VXLAN-kapsulointi lisää IP-pakettien kokoa. IP-pakettien koon kasvaminen taas aiheuttaa IP-pakettien pilkkomisen eli fragmentoinnin. Jotta voidaan välttyä ylimääräiseltä IP-pakettien pilkkomiselta, tulee MTU-arvon olla vähintään 1600.

Kuorman tasapainottamisen sääntönä tulee käyttää IP-paketin lähde- ja kohdeosoitteista laskettua tiivistettä (route based on IP-hash), sillä VLAN ei tue muita kuorman tasapainottamisen sääntöjä. Mikäli käytetään ryhmälähetystä ja VXLAN-liikenne

kulkee reitittimien välillä, tulee ryhmälähetys olla kytkettynä päälle reitittimissä. Vaihtoehtoina ovat PIM-BIDIR (Bidirectional Protocol Independent Multicast) ja PIM-SM toiminnot, joista PIM-BIDIR -toiminnon käyttö on suositeltavaa, mikäli se vain on valittavissa, sillä se mahdollistaa ESXi-isäntäpalvelinten toimia sekä lähettäjinä että vastaanottajina samanaikaisesti. [34, 35]

4.1.5 VCNI

VCNI (vCloud Network Isolation) on hieman VXLANia vastaava tapa yhdistää verkkoja. Samankaltaisuus löytyy kapsuloinnista ja kahden eri päätepisteen välille luotavasta tunnelista. VCNI:tä hallitaan vCloud Directorilla, joka käyttää ESXi-isäntäpalvelimiin asennettuja agentteja konfigurointiin. VCNI:n tarkoitus on yhdistää verkko siirtoyhteyskerroksella. VCNI toimii käyttämällä MAC-in-MAC kapsulointia tunneloidakseen liikenteen kahden ESXi-isäntäpalvelimen välillä VMkernel-moduulin läpi. ESXi-isäntäpalvelimet lisäävät alkuperäiseen Ethernet-kehykseen uuden otsakkeen ennen kuin kehys ohjataan fyysiselle verkkolaitteelle.

VCNI-verkon liikennöintiin käytetään dvSwitchiä. DvSwitchien välille luodaan oma VLAN-segmentti, jota käytetään kapsuloidun liikenteen välittämiseen. Myös VCNI-ominaisuutta voidaan täten overlay-teknologiaksi. Koska dvSwitchit luodaan vCloud Directorilla, antaa vCloud Director VLANia luodessa tälle eristetylle verkolle oman Network ID-numeron. ESXi-isäntäpalvelin kapsuloi siirrettävän datan ja lähettää sen dvSwitchien välille luotuun VLAN-segmenttiin. Uusi kehys sisältää kohteen ESXi-isäntäpalvelimen MAC-osoitteen, lähteen ESXi-isäntäpalvelimen MAC-osoitteen ja Network ID-numeron. Kun kehys saapuu kohteena olevan virtuaalisen tietokoneen ESXi-isäntäpalvelimelle, ESXi-isäntäpalvelin purkaa kehyksen ulomman otsakkeen ja ohjaa alkuperäisen kehyksen oikealle virtuaaliselle tietokoneelle.

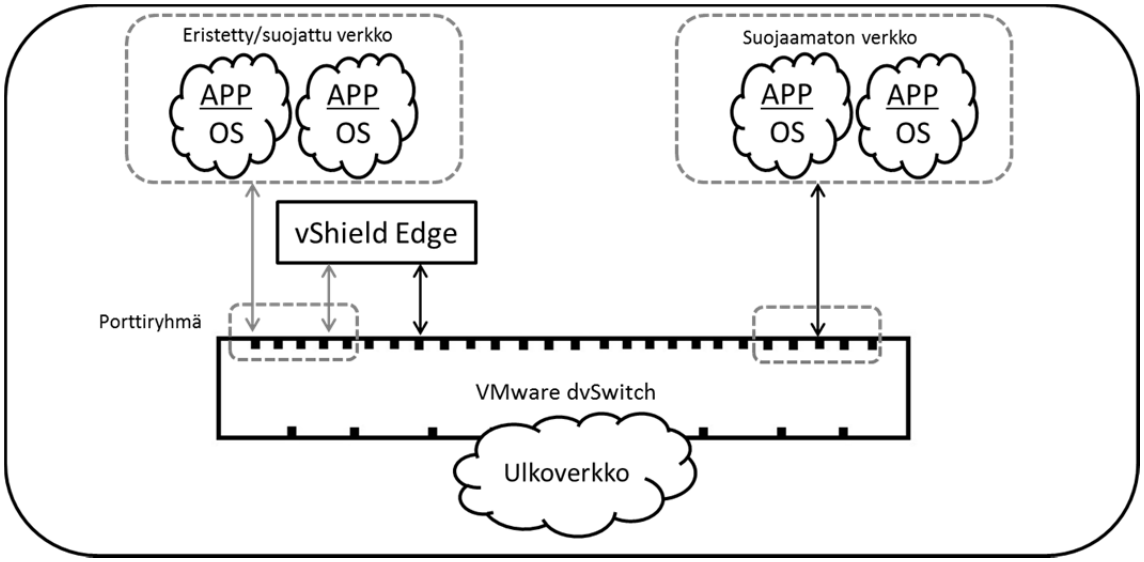
VCNI-verkkoa konfiguroitaessa tulee ottaa huomioon, että lisättäessä kehykseen uusi ulompi otsake, tulee fyysisten kytkinten MTU-arvoa kasvattaa normaalista 1500 tavusta 1524 tavuun. Lisäksi on otettava huomioon, että ESXi-isäntäpalvelin on ainoa, joka pystyy purkamaan kapsuloinnin, joten tämänkaltainen liikenne ei ole reititettävissä. Myös tässä toteutuksessa käytetyt virtuaaliset kytkimet tulee konfiguroida MTU-arvon osalta oikein. Jumbo-kehyksiä, joiden MTU on normaalisti 9000 tavua, käytettäessä tulee huomioida, että MTU-arvoa tulee pienentää 24 tavun verran. [36, s. 6-7]

4.1.6 vShield Edge

vShield Edge on VMwaren kehittämä yhdyskäytävä pilviympäristöön. Se on pilviympäristöön tehty tietoturva-ratkaisu. vShield Edge sisältää palomuurin ja sen lisäksi sen tärkeimmät ominaisuudet ovat NAT (osoitteenmuunnos), DHCP ja VPN. Tietoturva on nykyään yksi tärkeimmistä asioista tietoliikenteessä, varsinkin kun kyseessä on pilviympäristöt, joissa saattaa olla jopa tuhansia virtuaalisia asiakkaiden palvelimia. Tämän vuoksi VMwaren verkon avainkomponentteihin kuuluu vShield Edge, joka toimii yhdyskäytävänä ja palomuurina virtuaalisen kytkimen ja virtuaalisten tietokoneiden

välillä. Periaatteessa vShield Edge voidaan ajatella virtuaaliseksi palomuuritietokoneeksi, joka suodattaa liikennettä kytkimen ja virtuaalisten tietokoneiden välillä. Se erottaa virtuaaliset tietokoneet porttiryhmien avulla. vShield Edgeä voidaan hallita vCenter Serverin tai vCloud Directorin kautta. vCloud Directorin tapauksessa vShield Edge provisioidaan vAppina. Seuraavassa kuvassa (Kuva 11) on esitelty vShield Edgen looginen sijoitusmalli. Kuvasta nähdään, että vShield Edge liikennöi tiettyyn porttiryhmään kuuluvien tietokoneiden ja virtuaalisen kytkimen välillä.

vShield Edgeä voidaan käyttää kahdella eri tavalla. vShield Edge voidaan ottaa käyttöön Port Group Isolation -ominaisuutta käyttäen, mikä tarkoittaa sitä, että vShield Edge luo turvallisen ja eristetyn verkon pelkästään porttiryhmien avulla, käyttämättä verkon segmentoinnissa VLANeja. Tässä tapauksessa suojatussa verkossa olevat virtuaaliset tietokoneet voivat keskustella ainoastaan samassa porttiryhmässä olevien virtuaalisten tietokoneiden kanssa. Toinen vaihtoehto on käyttää VLANeja. Tässä tapauksessa virtuaaliset tietokoneet eristetään toisistaan ainoastaan VLANien avulla ja oikeiden VLAN-konfiguraatioiden tekeminen jää pilviympäristön ylläpitäjän vastuulle. Käytettäessä VLANeihin perustuvaa eristämistä voidaan virtuaalisina kytkiminä käyttää tavallista vSwitchiä, hajautettua dvSwitchiä tai Ciscon Nexus 1000V kytkintä. Eristettäessä verkko ainoastaan porttiryhmien avulla, käytettävissä on ainoastaan hajautettu dvSwitch. [37, s. 4-5]



Kuva 10: vShield Edgen looginen sijoitusmalli. [37, s. 4]

Palomuuri

vShield Edgen palomuuri tukee IP-pohjaisia 5-tuple konfiguraatiosääntöjä, jotka sisältävät lähteen ja kohteen IP-osoitteet, halutut porttivälit ja TCP, UDP sekä ICMP liikenteen suodatuksen. Koska palomuuriin voidaan määritellä suodatus lähde- ja kohdeporttien perusteella, se mahdollistaa esimerkiksi FTP- ja RPC-protokollien käytön, sillä nämä protokollat vaativat useita portteja tiedonsiirtoa varten. Mikäli porttisäännöillä ei erikseen sallita liikennettä, se estetään. [37, s. 5]

NAT (Network Address Translator)

Osoitteenmuunnos eli NAT on yksi tärkeimmistä vShield Edgen ominaisuuksista. Perinteisesti NAT on kehitetty ajatellen IPv4-osoitteiden rajallista määrää ja sen avulla voidaan yhtä ulkoista IP-osoitetta kohtaan määritellä useita sisäverkon osoitteita. vShield Edgen NAT toiminnon avulla voidaan toteuttaa lähteen ja kohteen IP-osoitteen sekä TCP- ja UDP-porttien perusteella tehtävä osoitteenmuunnos. Lähteen perusteella tehtävä osoitteenmuunnos muuttaa sisäisen suojatun aliverkon IP-osoitteen ulkoisen verkon julkiseksi IP-osoitteeksi ulospäin tapahtuvaa liikennöintiä varten ja kohteen perusteella tehtävä osoitteenmuunnos tekee saman sisään tulevalle liikenteelle. [37, s. 5]

DHCP (Dynamic Host Configuration Protocol)

vShield Edge sisältää myös DHCP-ominaisuuden. DHCP on verkkoprotokolla, jonka tärkein tehtävä on jakaa IP-osoitteita lähiverkkoon kytketyille tietokoneille eli tässä tapauksessa virtuaalisille tietokoneille. vShield Edgen DHCP:hen voidaan määritellä halutut IP-osoitealueet, yhdyskäytävä, DNS-palvelimet, haettavat domainit kuten myös staattisen IP-osoitteen antaminen tietyn MAC-osoitteen tai nimen omaavalle virtuaaliselle tietokoneelle. vShield Edgen DHCP kuuntelee sisäisen verkkorajapinnan puolelta tulevia DHCP-pyyntöjä ja antaa määritystensä mukaiselta IP-osoitealueelta uudelle verkkolaitteelle sisäisen IP-osoitteen sekä oman sisäisen verkkoliitännän mukaisen yhdyskäytävänä käytettävän IP-osoitteen. [37, s. 6]

Site-to-site VPN (Virtual Private Network)

VPN-yhteyttä käytetään kun halutaan luoda kahden pisteen välille virtuaalinen tunneli. VPN:n avulla ulkoverkossa oleva tietokone voi esimerkiksi yhdistää yrityksen sisäverkkoon ja saada näin käyttöönsä vain sisäverkkoon rajatut palvelut. vShield Edgen VPN käyttää standardisoituja protokollia ja asetuksia, jotka toimivat yhteen kaikkien suurimpien palomuurien valmistajien kanssa. vShield Edge VPN tukee myös IPSec VPN:ää. Lisäksi se tukee ennalta jaetun avaimen käyttöä, AES- tai 3DES-salausta, IP-täsmälähetys liikennettä ja staattista reititysprotokollaa itsensä ja VPN-reitittimien välillä. Jokaisen VPN-reitittimen taakse voidaan konfiguroida useita eri aliverkkoja yhdistymään vShield Edgen takana olevaan sisäverkkoon IPSec-tunneleiden avulla. [37, s. 6]

Muut ominaisuudet

Edellä mainittujen ominaisuuksien lisäksi vShield Edge sisältää Web Load Balancing- ja Remote Syslog -toiminnot. Web Load Balancingia käytetään jakamaan palvelinten kuormaa useammalle palvelimelle esimerkiksi siinä tapauksessa, että yksi web-sivustoa ylläpitävä palvelin kuormittuu liikaa. Remote Syslog -toiminnon avulla on taas mahdollista valvoa tiettyjä tapahtumia verkossa ja siirtää ne etänä lokipalvelimelle. [37, s. 6]

4.2 Microsoft ja lähiverkot

Microsoft on maailman suurin ohjelmistoalan yritys ja tämän vuoksi on täysin normaalia, että se kilpailee myös virtualisoinnin ja pilvipalveluiden alalla. Microsoftin päätavoite pilvipalveluiden avulla on optimoida yritysten liiketoimintaa. Virtualisoidut lähiverkot ovat osa pilvipalveluita ja Microsoftin kehittämät komponentit niiden toteuttamiseksi on esitelty seuraavaksi.

Microsoftin käyttämä hypervisor on nimeltään Hyper-V. Se julkaistiin alun perin stand-alone käyttöjärjestelmällä nimeltä Hyper-V Server. Windows Server 2008 -palvelinohjelmistosta lähtien se on kuitenkin asennettavissa myös Windows Server roolina. Microsoft käyttää palvelimeen asennettavista lisätoiminnallisuuksia tuovista ohjelmistoista nimitystä rooli ja niiden avulla Windows Serverin toiminnallisuutta voidaan laajentaa. Tässä työssä käytetään Hyper-V käyttöjärjestelmään viitatessa nimitystä Windows Server 2012 R2, joka on uusin palvelinohjelmisto Microsoftilta. Näin ollen oletuksena on, että Hyper-V Server rooli on asennettu Windows Server 2012 R2 -käyttöjärjestelmään.

4.2.1 System Center

Microsoft System Center on VMwaren vCloud Directoria vastaava tuote. Se mahdollistaa koko pilvipalvelujärjestelmän keskitetyn ja ketterän hallinnan eri pilvijärjestelmien välillä. Esimerkiksi kahden fyysisesti eri sijainnissa olevan pilvijärjestelmän yhdistetty hallinta onnistuu System Centerin avulla eikä ole merkitystä onko kyseessä julkinen, yksityinen pilvi vai hybridipilvi. System Centerin tärkeimmät ominaisuudet ovat koko infrastruktuurin laajuinen provisiointi ja valvonta, automaation ja itsepalvelun toteuttaminen, sovelluskohtainen suorituskyvyn valvonta ja ylläpidon hallinta. Koko infrastruktuurin laajuisella provisioinnilla tarkoitetaan esimerkiksi mahdollisuutta luoda virtuaalisia tietokoneita mihin tahansa System Centerin alaisista pilvijärjestelmistä. Valvonnan avulla pystytään seuraamaan kaikkia infrastruktuurin fyysisiä ja virtuaalisia laitteita sekä koko pilvijärjestelmää. Automaation ja itsepalvelun toteuttamisella tarkoitetaan sitä, että sovellusten omistajat eli esimerkiksi palvelinsovellusta pilvijärjestelmässä ylläpitävät henkilöt voivat itse pitää huolta oman sovelluksensa toimivuudesta jättäen itse infrastruktuurista huolehtimisen pilvipalvelujärjestelmän ylläpitäjille. Sovelluskohtaisella suorituskyvyn valvonnalla pilvipalvelun asiakkaat ja ylläpitäjät voivat valvoa kuinka paljon sovellukset käyttävät resursseja ja esimerkiksi mikä niiden käyttöaste on sekä määrittää erilaisia automatisoituja toimenpiteitä jotka tapahtuvat esimerkiksi sovelluksen kuormituksen kasvaessa.

System Center koostuu useista yhteen kootuista hallintaohjelmista. Ne ovat System Orchestrator, Service Manager, Virtual Machine Manager, Configuration Manager, Operations Manager ja Data Protection Manager. System Centerin kautta pystyy siis hallitsemaan kaikkien näiden hallintaohjelmistojen toimintoja.

Tärkeimmäksi asiaksi jatkuvasti kehittyvillä markkinoilla ja niiden mukana pysymisessä Microsoft mainitsee ketteryyden. Tämän vuoksi se on kehittänyt System Cen-

terin, jonka avulla pystytään hallitsemaan isojakin kokonaisuuksia pilvipalvelujärjestelmistä. System Center ei ole ainoastaan pilvipalvelujärjestelmän ylläpidolle suunnattu, vaan myös sen sovelluskohtaisille asiakkaille suunnattu järjestelmä, jonka tarkoitus on nopeuttaa ja helpottaa omaa liiketoimintaa. [38]

4.2.2 Hyper-V Extensible Switch

Microsoft tarjoaa verkon virtualisointiin käytettäväksi Hyper-V Extensible Switchin. Hyper-V Extensible Switch nimitys korostaa sen laajennettavuutta, mutta siitä käytetään myös nimitystä Hyper-V Virtual Switch. Tässä työssä Microsoftin virtuaalisesta kytkimestä käytetään jatkossa lyhennettä ES. ES on ohjelmallisesti toteutettu siirtokerroksen verkkokytkin, joka on käytettävissä Hyper-V Managerin asennuksen jälkeen. Hyper-V Manager on isäntäpalvelimeen eli Windows Server 2012 R2:aan asennettava hallintaohjelmisto. ES sisältää ohjelmallisesti hallittavia ja laajennettavia ominaisuuksia, joiden avulla virtuaaliset tietokoneet voidaan yhdistää virtuaalisiin ja fyysisiin verkkoihin. Lisäksi ES tarjoaa käytettäväksi tietoturvaan, eristykseen ja palvelutasoihin liittyviä sääntöjä. ES sisältää myös mahdollisuuksia käyttäjien eristykseen, verkkoliikenteen muokkaamiseen, suojautumiseen uhkaavia virtuaalisia tietokoneita kohtaan sekä yksinkertaistetun vianmäärityksen.

Sisäänrakennetun NDIS-suodatusajureiden (Network Device Interface Specification) ja WFD-kutsuajureiden (Windows Filtering Platform) avulla ES tarjoaa myös itsenäisille ohjelmistokehittäjille mahdollisuuden luoda kytkimeen lisäosia, joiden avulla voidaan parantaa liikennöintiä ja tietoturvaa.

Looginen verkkotopologia, joka muodostetaan ES:n avulla, on täysin vastaava VMwaren vSwitchillä muodostettuun ja se on esitetty luvussa 4.1.2 (Kuva 3). Vaikka looginen kuva onkin vastaava, on näillä kytkimillä joitakin eroja, kuten porttien määritykset ja verkkoadapterit. [39]

Portit

Microsoft määrittelee ES:ssä portit kahteen eri kahteen eri kategoriaan, varmistusportteihin (validation ports) ja toiminnallisiin portteihin (operational ports). Varmistusportit ovat väliaikaisia portteja, joiden avulla varmistetaan verkkoon kytkettävän tietokoneen verkkoasetukset ja toiminta ennen kuin varsinainen liikennöinti alkaa. Varmistusportti luodaan samalla kun virtuaalinen tietokone luodaan ja se poistetaan kun virtuaalinen tietokone kytketään päälle, jolloin sen tilalle luodaan toiminnallinen portti, joka vastaa varsinaisesta liikennöinnistä.

Kun virtuaalinen tietokone luodaan, varmistusportit pyytävät sille kuuluvat asetukset OID-pyynnöillä hallintaohjelmistolta. Varmistusportit tarkistavat seuraavat asiat: syntaksin tarkistus, alueen tarkistus, sopivuuden tarkistus ja ristiriitojen tarkistus. Syntaksin tarkistuksessa varmistusportti tutkii, ovatko konfiguraatioarvot oikealla tavalla kirjoitetut eli tarkistavat asetusten syntaksin. Alueen tarkistuksessa varmistusportit tarkistavat ovatko asetuksiin määritetyt arvot niille rajatuilla arvoalueella. Sopivuuden

tarkistuksessa varmistusportit tarkistavat esimerkiksi sen, että ovatko portille määritetyt säännöt mahdollista toteuttaa. Tällainen tilanne voi olla esimerkiksi silloin kun virtuaaliselle tietokoneelle on määritetty yhteys ulkoverkkoon vaikka VS ei olisi edes kytketty siihen. Ristiriitojen tarkistus varmistaa porttiin määritetyt asetukset eivät ole ristiriidassa keskenään. Varmistusporttien tärkein tehtävä on siis yhteyden toiminnallisuuden varmistaminen ja vianrajaus jo ennen kuin virtuaalinen tietokone kytketään verkkoon.[40]

Toiminnalliset portit ovat liikennöintiä varten luotuja portteja. Kun toiminnallinen portti luodaan, sille määritetään porttityyppi. Tämä määritetty porttityyppi pysyy aktiivisena kunnes se suljetaan eli esimerkiksi silloin kun virtuaalinen tietokone sammutetaan. Toiminnallisten porttien porttityypit määrittelevät sen, millainen verkkoadapteri siihen voidaan kytkeä. Porttityyppi määrittelee siis sen, onko verkkoadapteri fyysinen ulkoverkkoon kytketty verkkoadapteri vai virtuaalinen verkkoadapteri, joka voi olla sisäinen, synteettinen tai emuloitu External-porttityypin eli ulkoisen porttityypin avulla määritetään ulkoverkkoon yhdistettävä portti. Tämä tarkoittaa siis sitä, että ulkoiseen porttityyppiin kytketään fyysinen verkkoadapteri, joka sijaitsee Hyper-V isäntäpalvelimessa ja jolla on pääsy ulkoiseen verkkoon. Porttityyppiä määritellessä on tärkeää huomioida, että ES:ssä voi olla ainoastaan yksi ulkoiseksi porttityypiksi määritetty portti. Tämä tarkoittaa siis sitä, että VS:ssä on ainoastaan yksi ulkoverkon suuntaan liikennöivä kytkinportti kun taas esimerkiksi VMwaren vSwitchissä ylälinkkiportteja voi olla useita. Internal-porttityypin eli sisäisen porttityypin avulla määritetään sisäverkkoon yhdistettävä portti. Tätä porttityyppiä käytetään kun yhdistetään VS sisäverkkoon. Tämä tarkoittaa sitä, että sisäverkkoon yhdistetyn portin kautta hoidetaan esimerkiksi verkon ja virtuaalisten tietokoneiden hallinnointiliikenne. Tämän portin kautta hallintaohjelmisto saa yhteyden virtuaaliseen kytkimeen. Myös sisäisen porttityypin kohdalla tulee huomioida, että VS tukee ainoastaan yhtä sisäiseksi porttityypiksi määritettyä porttia ja näin ollen vain yhtä hallinnalle määritettyä liikennöintiväylää. Ulkoisen ja sisäisen porttityypin lisäksi on vielä Synthetic- ja Emulated-porttityypit eli synteettinen ja emuloitu porttityyppi. Näitä porttityyppejä käytetään porteissa, joihin kytketään virtuaaliset tietokoneet. Synteettistä porttityyppiä käytetään virtuaalisissa tietokoneissa, joihin asennetaan Windows Vista tai sitä uudempi käyttöjärjestelmä ja emuloitua porttityyppiä käytetään niissä virtuaalisissa tietokoneissa, joihin asennetaan Windows XP tai jokin muu käyttöjärjestelmä kuin Windows. [41]

Verkkoadapterit

Kuten ”Portit”-alaluvussa kerrottiin, ES tukee yhteyksiä useilta fyysisiltä ja virtuaalisilta verkkoadaptereilta. External- eli ulkoiset verkkoadapterit ovat isäntäpalvelimeen asennettavia fyysisiä verkkoadaptereita, jotka tarjoavat yhteyden ulkoverkon suuntaan. Ulkoisen verkkoadapterin asetuksia voidaan hallita fyysisen isäntäpalvelimen kautta. Ulkoisen verkkoadapterin yhteyttä voivat hyödyntää kaikki child partitionit, jotka ovat kytkettynä samaan ES:ään kuin ulkoinen verkkoadapteri. Microsoft erottelee virtuaaliset tietokoneet ja fyysiset isäntäpalvelimet nimillä child partition ja parent partition. Ulkoinen verkkoadapteri on virtuaalinen esitysmuoto sen alla olevasta fyysisestä verkkoadap-

terista, joka on fyysisesti kytketty Hyper-V -isäntäpalvelimeen. Ulkoinen verkkoadapteri ohjaa eteenpäin OID-pyyntöjä ja NDIS-tilailmoituksia yhdelle tai useammalle sen alla toimivista fyysisistä verkkoadaptereista. Vaikka yksi ES tukee vain yhtä ulkoista verkkoadapteria, se ei siis tarkoita, että fyysisessä Hyper-V -isäntäpalvelimessa ei voisi olla useampia fyysisiä verkkoadaptereita, jotka on esimerkiksi ryhmitetty yhteen. Sisäisesti eli ES:n kannalta ajateltuna ulkoinen verkkoadapteri sitoutuu useisiin sen alla toimivien fyysisten verkkoadaptereiden konfiguraatioihin, kuten LBFO-team eli LBFO-ryhmä (Load Balancing and Failover). LBFO-ryhmä on NDIS-suodatusajuri, joka voi olla ryhmitetty yhteen tai useampaan fyysiseen verkkoadapteriin. Jokainen näistä konfiguraatioista tarjoaa yhteyden ulkoverkkoon joko yhden tai useamman fyysisen verkkoadapterin kautta. Ulkoisten verkkoadaptereiden konfiguraatioihin kuuluu lisäksi myös NDIS MUX -ajuri, joka on myös sidottu ryhmään, johon kuuluu yksi tai useampi fyysinen verkkoadapteri. [42, 43]

Internal- eli sisäinen verkkoadapteri on hallintaa varten käytetty verkkoadapteri. Sen avulla Hyper-V -isäntäpalvelin pystyy lähettämään ja vastaanottamaan paketteja ES:n kautta. Koska sisäinen verkkoadapteri on hallintaan käytetty verkkoadapteri, jota ei ole kytketty mihinkään fyysiseen verkkoadapteriin, se on virtuaalinen verkkoadapteri. Se ei kuitenkaan toimi varsinaisesti emuloiden mitään tiettyä verkkoadapteria, vaan se on Microsoftin oma nimenomaisesti hallintaa varten oleva verkkoadapteri. [44]

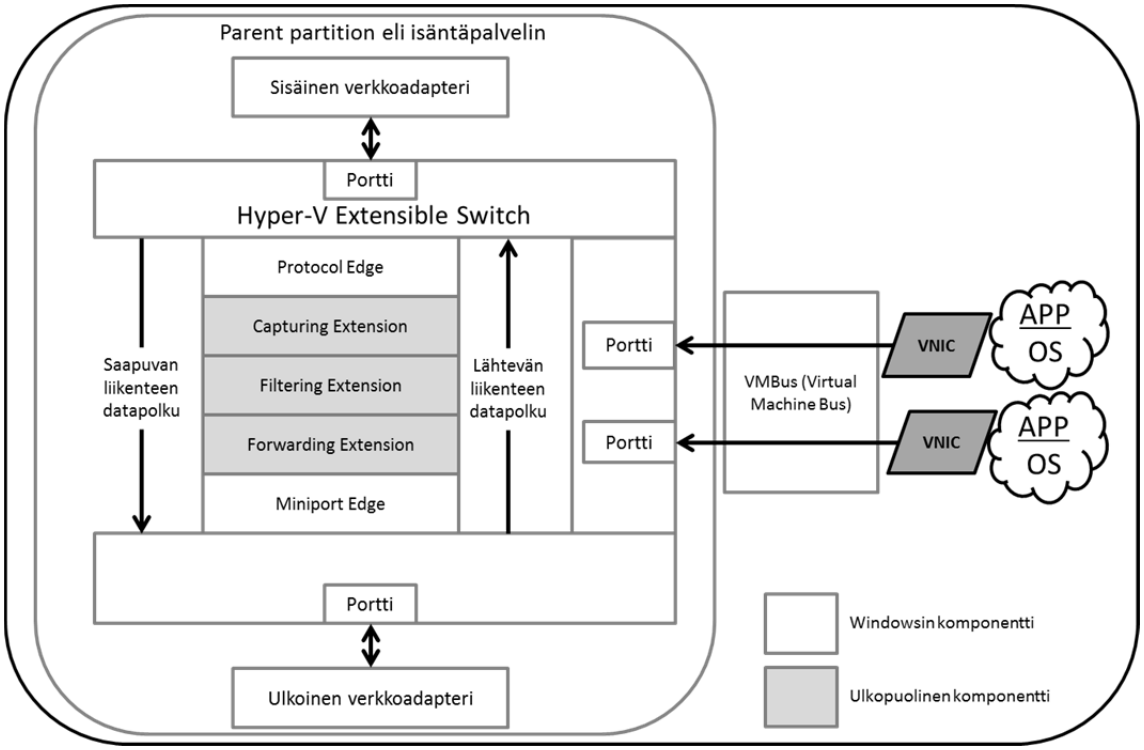
Virtuaalisten tietokoneiden verkkoadapterit ovat kytkettyinä child partitioneihin eli virtuaalisiin tietokoneisiin. Microsoft on kehittänyt ES:ään kaksi vaihtoehtoista virtuaalista verkkoadapteria: synteettisen ja emuloidun verkkoadapterin. Molemmat verkkoadapterit kuljettavat liikenteen VMBus-väylää pitkin virtuaaliselle kytkimelle. VMBus on siis loogisesti ajateltuna virtuaalisen tietokoneen ja kytkimen välillä oleva verkkokaapeli. Synteettinen verkkoadapteri toimii NetVSC:n avulla. NetVSC (Network virtual service client) on periaatteessa siis virtuaalisen verkkoadapterin toiminnallisuuden sisältävä osa. Emuloitu verkkoadapteri toimii hieman eri tavalla sillä se matkii Intel-pohjaisen verkkoadapterin toimintaa. Emuloidun verkkoadapterin avulla siis virtuaalinen tietokone kuvittelee sen verkkoadapterin olevan Intelin valmistama fyysinen verkkoadapteri.[45]

Extensible Switchin toiminta

ES:n avulla virtualisoidussa verkossa paketit kulkevat joko datapolkua (Data Path) ja hallintapolkua (Control Path) pitkin. Kuten nimistä voi päätellä, datapolkua käytetään virtuaalisten tietokoneiden datan kuljettamiseen ja hallintapolkua hallintayhteyden dataa varten.

Kaikki paketit, jotka saapuvat virtuaaliseen kytkimeen sen porttien kautta, kulkevat samaa reittiä virtuaalisen kytkimen sisällä. Esimerkiksi ulkoisesta verkkoadapterista tulleet ja virtuaalisesta tietokoneesta lähetetyt paketit kulkevat samaa reittiä. Pakettiliikenne kulkeutuu ES:n läpi seuraavalla tavalla: paketit saapuvat ES:ään verkkoadaptereista, jotka ovat kytkettynä sen portteihin. Näitä paketteja käsitellään ensimmäiseksi lähetyspyyntöinä ja ne ohjataan ajuripinon läpi. Tätä polkua kutsutaan saapuvan liiken-

teen datapoluksi. ES koostuu ohjelmallisesti viidestä eri osasta: ES Protocol Edge -osiosta, Capturing Extensions -osiosta, Filtering Extensions -osiosta, Forwarding Extensions -osiosta ja ES Miniport Edge -osiosta. Protocol Edge ja Miniport Edge ovat Windowsin omia komponentteja ja loput ovat kolmannen osapuolen eli ulkopuolisen kehittäjän tekemiä ES:n laajennusosia. Protocol Egde -osio valmistaa porteista saapuvat paketit kulkemaan saapuvan liikenteen polkua pitkin lisäämällä niihin alueen OOB-tiedoille. OOB-tiedot (out-of-band) sisältävät eteenpäinohjaukseen tarvittavat tiedot. Se sisältää tiedot lähdeportista ja verkkoadapterista, jota käytettiin paketin lähettämisessä ES:lle. Protocol Edge -osio lisää OOB-tietoihin kuitenkin ainoastaan lähdeportin ja virtuaalisen tietokoneen verkkoadapterin tiedot Seuraavaksi Extensions- eli laajennus-osiot ottavat paketin käsittelyynsä saapuvan liikenteen datapolulta. Riippuen laajennus-osiosta, ne voivat joko hylätä paketin tai ohjata sen eteenpäin. Esimerkiksi Filtering- ja Forwarding-osiot voivat tiputtaa paketin, mikäli se ei ole niiden sääntöjen mukainen. Capturing Extensions -osio voi myös ottaa saapuneen paketin käsittelyynsä ja tutkia sen sisältämää dataa, mutta sillä ei ole oikeutta hylätä tai ohjata pakettia eteenpäin niin, että se kulkisi suoraan sen loppupäämäärään, vaan sen tulee aina ohjata paketti joko Filtering- tai Forwarding-osiolle. Capturing Extensions -osiolla voi kuitenkin luoda paketteja saapuvan liikenteen datapolulle. Tämä voi tapahtua esimerkiksi silloin, kun sen avulla valvotaan verkkoliikenteen tilaa ja raportit lähetetään etänä toimivalle valvontasovellukselle. Kun paketti saapuu Filtering Extensions -osiolle, osio voi suorittaa seuraavat toimenpiteet: hylätä paketin kytkimen tai porttien sääntöjen perusteella, kloonata tai muokata pakettia tai luoda uusia paketteja lähetettäväksi saapuvan liikenteen datapolulle. Forwarding Extensions -osiolla on tärkeä tehtävä kytkimen toiminnallisuuden kannalta. Se lisää Protocol Edgen -tekemään OOB-tietoon paketin kohdeportit. ES voi kuitenkin toimia ilman Forwarding Extensions -osiota, jolloin OOB-tietoon lisätään kohdeportit saapuvan liikenteen datapolun päätepisteessä eli Miniport Edgessä. Kuten Filtering Extensions -osio, voi myös Forwarding Extensions -osio hylätä paketteja sääntöjen perusteella. Kytkimen ja porttien säännöt sisältävät sääntöjä liittyen tietoturvallisuuteen ja VLAN-ominaisuuksiin. Lisäksi myös Forwarding Extensions -osio voi kloonata, muokata tai luoda uusia paketteja saapuvan liikenteen datapolulle. Paketti on Extensions-osioiden jälkeen kulkeutunut saapuvan liikenteen datapolun päätepisteeseen eli Miniport Edgeen. Miniport Edge on viimeinen osio ennen kuin paketti voidaan ohjata ulkoista verkkoadapteria pitkin sen kohteeseen tai mikäli paketin kohde on samassa virtuaalisessa kytkimessä sijaitseva virtuaalinen tietokone, paketti ohjataan lähtevän liikenteen datapolulle. Myös ulkoverkosta tulleet paketit ohjataan Miniport Edgen toimesta saapuvan liikenteen datapolulle. Saapuvan liikenteen datapolku on toiminnallisesti täysin vastaava kuin lähtevän liikenteen datapolku, paketit vain kulkevat toiseen suuntaan. Tämä tarkoittaa sitä, että myös saapuvan paketit käyvät ajuripinossa olevat osiot läpi ja ne voidaan esimerkiksi hylätä tai niitä voidaan valvoa. Miniport Edgen avulla voidaan toteuttaa myös portin peilaus (port mirroring). Mikäli portin peilaus on asetettu päälle, Miniport Edge lisää paketin OOB-tietoihin kohdeportin, johon peilaus toteutetaan. Microsoft Hyper-V Extensible Switchin toiminta on esitetty seuraavassa kuvassa (Kuva 11). [46]



Kuva 11: Microsoft Hyper-V Extensible Switchin arkkitehtuuri.

Control pathia eli hallintapolkua pitkin kuljetetaan OID-pyynnöt ja NDIS-tilailmoitukset ES:lle. OID-pyynnöillä isäntäpalvelin ilmoittaa virtuaaliselle kytkimelle uudet tai muuttuneet asetukset koskien kytkimen portteja ja sen virtuaalisia verkkoadaptereita. Lisäksi OID-pyynnöillä ilmoitetaan kytkimeen tai sen portteihin liittyvistä muutoksista. Nämä OID-pyynnöt ovat tärkeitä kytkimen toiminnan kannalta ja kytkimessä olevien Filtering- ja Forwarding Extensionien tulee sallia näiden pakettien pääsy Miniport Edgeen asti, sillä Miniport Edgen on saatettava halutut muutokset voimaan niin sanotusti kuittaamalla OID-pyynnöt. OID-pyynnöt aloittaa Protocol Edge -osio ja se ilmoittaa ne nimenomaisesti Filtering- ja Forwarding -osioille, joihin muutokset tulevat. OID-pyynnöt kulkevat siis kytkimen koko ajuripinon läpi. OID-pyynnöt kulkeutuvat loogisesti samaa reittiä kuin saapuvan liikenteen data eli sisäiseltä verkkoadapterilta kohti Miniport Edge -osiota ja siihen asti. [47]

NDIS-tilailmoitukset kulkevat ES:ssä eri suuntaan kuin OID-pyynnöt, sillä ne tulevat ulkoiselta fyysiseltä verkkoadapterilta. Ne siis kulkevat loogisesti samaa väylää kuin saapuvan liikenteen data. NDIS-tilailmoituksia käytetään esimerkiksi tilanteessa, jossa useita fyysisiä verkkoadaptereita on ryhmitetty yhteen ja virtuaalisen kytkimen tulee tietää näistä muutoksista ja siitä mihin se ohjaa paketteja. Kun useita fyysisiä verkkoadaptereita on ryhmitetty yhteen ja ES:ssä ulkoinen verkkoadapteri on sidottu useampaan ulkoverkkoon, tulee ES:n Filtering- ja Forwarding-osioiden tietää tästä, jotta ne voivat ohjata paketit oikeaan suuntaan. Lisäksi Forwarding-Extensionin avulla voidaan hallita yksittäisten verkkoadaptereiden toimintaa ryhmityksessä. Tämä on aiheellista esimerkiksi silloin kun Hyper-V pilvijärjestelmässä halutaan käyttää LBFO-

ominaisuutta. LBFO:ta käytetään kuormituksen hallintaan ja failover-tukeen ja se toteutetaan erillisellä teaming provider -laajennuksella, joka on asennettavissa ES:ään. [48]

Tallennus- ja palautustoiminnot

Microsoft on kehittänyt virtualisoidun verkon vikasietoisuuden parantamiseksi tallennus- ja palautus -toiminnot (Save and Restore Operations). Näiden toimintojen avulla ES:ään kytketty virtuaalinen tietokone pystyy esimerkiksi jatkamaan toimintaansa toisella isäntäpalvelimella ilman käyttökatkoa. Kun Hyper-V child partition eli virtuaalinen tietokone sammutetaan, tallennetaan tai sille suoritetaan reaaliaikainen migraatio, sen suoritustila tallennetaan. Tämän tallennusoperaation aikana ES:ään asennettu laajennus voi tallentaa myös verkon suoritus tilan ja näin ollen kun virtuaalinen tietokone taas käynnistetään, se voi jatkaa tarkalleen siitä mihin se jäi. Kun virtuaalinen tietokone siirretään toiseen isäntäpalvelimeen, sen suoritustila ja verkkoasetukset säilyvät eikä verkkoyhteyttä katkaista ES:n toimesta missään vaiheessa. Kun palautusvaihe suoritetaan, ES:n laajennus siirtää verkkoadapterin suoritustilan ja asetukset uudelle verkkoadapterille ja liikennöinti voi jatkua samasta tilanteesta, johon virtuaalinen tietokone jäi aikaisemmin. Tallennus- ja palautustoimintoa voidaan käyttää myös tilanteissa, joissa vikatilannetta ei ole eli virtuaalinen tietokone ja sen toiminta halutaan vain siirtää toiseen isäntäpalvelimeen. Tämä on manuaalisempi tapa, sillä alkuperäinen virtuaalisen tietokoneen tila ja verkkoasetukset tallennetaan halutussa vaiheessa ja sen toimintaa jatketaan toisessa isäntäpalvelimessa silloin kun virtuaalinen tietokone kytketään siellä päälle. Tallennus- ja palautustoiminnot eivät siis varsinaisesti tarvitse vikatilannetta, jotta niitä voidaan käyttää. [49]

Tietoturva

ES:ssä tietoturva voidaan toteuttaa usealla tavalla. Virtuaalisiin tietokoneisiin voidaan asentaa omat palomuurisovellukset tai esimerkiksi käyttää niissä käyttöjärjestelmien omia palomuureja ja virustorjuntaohjelmistoja. Toinen vaihtoehto on käyttää ES:n ominaisuuksia tietoturvan parantamiseksi. ES:ssä tämä voidaan toteuttaa kahdella eri tavalla: itse ES:n ACL-toiminnolla tai kolmannen osapuolen tekemien laajennusten kautta. Laajennusten on tietysti tuettava Microsoft Extensible Switchiä, jotta niitä voi käyttää sen kanssa.

ES:n ACL-ominaisuudet eli Access Control List -ominaisuudet tarjoavat ylläpitäjille mahdollisuuden suojata ES:ään kytkettyjä virtuaalisia tietokoneita palomuurisuojauksella ja vahvistetuilla säännöillä. Koska porttikohtaiset ACL:t konfiguroidaan ES:n kautta, niiden avulla on mahdollista hallinta kaikkien siihen liitettyjen virtuaalisten tietokoneiden tietoturvasääntöjä. ACL:n palomuurisääntöihin voidaan määritellä lähteen ja kohteen MAC-osoitteet, IP-osoitteet, protokolla, lähde- ja kohdeportit sekä lisäksi jokaiseen sääntöön voidaan erikseen määritellä koskeeko se lähtevää vai tulevaa liikennettä sekä hyväksytäänkö vai hylätäänkö paketti. ACL-palomuurisäännöt voidaan konfiguroida Windows PowerShellin kautta, joka on komentokehotepohjainen hallintaoh-

jelmisto. ES:n ACL-ominaisuus on yhteensopiva Hyper-V Network Virtualizationin kanssa, joka esitellään omassa alaluvussaan. [50]

Toinen vaihtoehto tietoturvan takaamiseksi virtuaalisille tietokoneille ES:n avulla on käyttää kolmannen osapuolen tekemää laajennosta. Tällöin ES:n ajuripinoon lisätään laajennos, joka toimii palomuurina. Esimerkiksi 5nine Software tarjoaa 5nine Cloud Security -palomuurin, joka on suunniteltu nimenomaan Hyper-V Extensible Switchille. [51]

Hyper-V -isäntäpalvelin voidaan myös suojata palomuurilla käyttämällä sen käyttöjärjestelmän eli Microsoft Server 2012 R2:n omaa palomuuria. Käytettäessä tätä palomuuria on kuitenkin tärkeä ymmärtää, että isäntäpalvelimen oma palomuuri suojaa ainoastaan isäntäpalvelimen, ei siihen asennettuja virtuaalisia tietokoneita. [52]

Dynaaminen verkkoliikenteen kuormantasaus

Verkkoliikenteen kuormantasauksesta Microsoft käyttää nimitystä LBFO. Se kutsuu sitä myös nimellä NIC teaming eli verkkoadaptereiden ryhmitys. Verkkoadaptereiden ryhmitys voidaan Windows Server 2012 R2:ssa tehdä joko fyysisille verkkoadaptereille tai virtuaalisille verkkoadaptereille. Verkkoadaptereiden ryhmityksen tarkoitus on mahdollistaa kaistanleveyden aggregointi ja failover eli verkon vikatilanteesta toipuminen. Ryhmitys vaatii vähintään yhden fyysisen verkkoadapterin olemassaolon, jota voidaan käyttää liikenteen erotteluun VLANien avulla tai mikäli halutaan käyttää failover-ominaisuutta, tulee käytössä olla vähintään kaksi fyysistä verkkoadapteria. Windows Server 2012 R2:lla on mahdollista ryhmittää 32 verkkoadapteria. Käytännössä ryhmitys tapahtuu niin, että kaksi tai useampi verkkoadapteri ryhmitetään ja esitetään tämän jälkeen käyttöjärjestelmälle yhtenä tai useampana virtuaalisena verkkoadapterina.

Ryhmitykseen käytetään kahdentyyppisiä algoritmeja: algoritmeja, jotka vaativat kytkimen osallistumisen ryhmitykseen ja algoritmeja, jotka eivät vaadi kytkimen osallistumista ryhmitykseen. Ensimmäisessä tapauksessa algoritmit usein vaativat, että kaikki verkkoadapterit on kytketty samaan kytkimeen. Toisessa tapauksessa tämä ei ole tarpeellista, koska kytkin ei tiedä kuuluvatko siihen kytketyt verkkoadapterit ryhmitykseen vai eivät. Kaksi yleisesti käytettyä ryhmitystapaa on staattinen ryhmitys (static teaming) ja dynaaminen ryhmitys (dynamic teaming). Staattinen ryhmitys vaatii kytkimen ja tietokoneen konfiguroinnin, jotta ne tietävät mitkä linkit muodostavat ryhmityksen. Staattisessa ryhmityksessä mikään protokolla ei avusta kytkintä tai tietokonetta tunnistamaan mahdollisia kaapelin irtoamisia tai muita virheitä, mitkä aiheuttavat ryhmityksen hajoamisen. Dynaamisessa ryhmityksessä käytetään LACP-protokollaa dynaamisesti tunnistamaan linkit tietokoneen ja tietyn kytkimen välillä. LACP-protokolla mahdollistaa automaattisen ryhmityksen luomisen ja teoriassa sen laajennuksen ja pienennyksen vain LACP-protokollan kuittausten avulla. Dynaaminen ryhmitys vaatii tietysti kytkimeltä LACP-protokollan tuen. Sekä staattisen että dynaamisen ryhmityksen tarkoituksena on saavuttaa useiden linkkien aggregoitu kaistanleveys, koska ryhmitetyt verkkoadapterit näkyvät loogisesti yhtenä.

Lähtevä liikenne voidaan jakaa saatavilla olevien linkkien avulla monella tavalla. Päätavat liikenteen jakamiselle ovat Hyper-V kytkimen porttiin perustuva liikenteen jakaminen ja tiivisteeseen perustuva jakaminen. Kytkimen porttiin perustuvassa liikenteen jakamisessa virtuaalisen tietokoneen MAC-osoite antaa perustan liikenteen jakamiselle. Tästä on apua virtualisointia käytettäessä, koska lähinnä oleva kytkin tunnistaa, että tietty lähdeosoite on kytketty ainoastaan yhteen verkkoadapteriin, pystyy kytkin tasapainottamaan kuorman kytkimeltä tietokoneelle useiden linkkien kautta, käyttäen virtuaalisen tietokoneen kohdeosoitetta. Tämä tapa liikenteen jakamiseen ei kuitenkaan välttämättä ole riittävän tarkkaa, jotta sillä saavutettaisiin hyvin tasapainotettu jakaminen ja se rajoittaa yhden virtuaalisen tietokoneen kaistanleveyden siihen, mitä yhdestä verkkoadapterista on saatavilla. Tiivisteeseen perustuvassa liikenteen jakamisessa liikenne jaetaan perustuen paketin komponenteista laskettuun tiivisteeseen. Kun tiiviste on laskettu, ohjataan samalla tiivisteellä olevat paketit aina samaan verkkoadapteriin. Tiivisteen laskemista varten käytetylle funktiolle voidaan antaa liikennepaketin komponenteista seuraavat arvot: lähteen ja kohteen MAC-osoitteet, lähteen ja kohteen IP-osoitteet joko MAC-osoitteiden kanssa tai ilman ja lähde ja kohde TCP-portit, joita usein käytetään yhdessä IP-osoitteiden kanssa. Tiivisteeseen perustuva liikenteen jakaminen johtaa yleensä hyvin tasapainoiseen liikenteen jakoon verkkoadaptereiden kesken.

Verkkoadaptereiden ryhmitys toimii myös virtuaalisissa tietokoneissa. Tämän ansiosta virtuaalisella tietokoneella voi olla useampia virtuaalisia verkkoadaptereita, jotka ovat kytkettyinä useampaan kuin yhteen ES:ään ja näin ollen sillä on varayhteys, mikäli toisen ES:n alla oleva fyysisen verkkoadapterin yhteys katkeaa. Tämä on hyvin tärkeä ominaisuus varsinkin käytettäessä SR-IOV:ia, sillä sitä käytettäessä liikenne ei kulje ES:n läpi ja tämän vuoksi sitä ei voida suojata ES:n alla olevalla fyysisten verkkoadaptereiden ryhmityksellä. Virtuaalisten verkkoadaptereiden ryhmityksen avulla ylläpitäjä voi kytkeä virtuaaliseen tietokoneeseen kaksi ES:ää, joiden molempien alla on SR-IOV:ta tukevat verkkoadapterit. Näin virtuaalisen tietokoneen liikenne on kahdennettu ja liikenne voi ensisijaisen yhteyden katketessa siirtyä toissijaiseen yhteyteen. [53]

Muita toiminnallisuuksia

Virtuaaliseen järjestelmään voidaan toteuttaa myös DHCP-palvelin Windows Server 2012 R2:n avulla. Koska Hyper-V on asennettu Windows Server 2012 R2:een roolina, on sen käytettävissä myös muita siihen asennettuja rooleja. Tässä tapauksessa itse isäntäpalvelin toimii samalla DHCP-palvelimena. DHCP-palvelimen voi toteuttaa myös virtuaalisella tietokoneella asentamalla virtuaaliselle tietokoneelle esimerkiksi oman Windows Server 2012 käyttöjärjestelmän ja konfiguroimalla DHCP-palvelimen siihen. Toinen vaihtoehto on asentaa virtuaaliselle tietokoneelle tai isäntäpalvelimelle RRAS-palvelinrooli (Routing and Remote Access Service). RRAS-palvelinroolin avulla on mahdollista toteuttaa erilaisia reititykseen ja etähallintaan liittyviä toimintoja kuten NAT, VPN ja DHCP. RRAS-palvelua käytettäessä on kuitenkin huomioitava, että sen toiminnallisuudet pätevät vain sen taakse kytkettyihin tietokoneisiin. [54, 55]

Hyper-V Extensible Switch sisältää lisäksi yhden tärkeimmistä ominaisuuksista SDN-konseptin kannalta, OpenFlow-tuen. Japanilainen NEC Corporation on nimittäin kehittänyt Extensible Switchiin ohjelmiston, joka on käytettävissä ES:n ajuripinon laajennusten kautta. OpenFlow-protokolla esitellään tarkemmin luvussa 6. [56]

4.2.3 Hyper-V Network Virtualization

Hyper-V Network Virtualization eli HNV on uusimmassa Windows Server 2012 R2 -versiossa julkaistu teknologia, jonka avulla organisaatio voi toteuttaa oman verkon segmentointia tai ulottaa sen esimerkiksi ulkoistuskumppanin tiloihin. Se tarjoaa siis vastaavanlaisia hyötyjä kuin VMwaren VXLAN-ominaisuus, mutta hieman eri tavalla. Hyper-V Network Virtualizationin tavoite on tehdä sama asia verkoille kuin hypervisorit tekevät tietokoneille eli virtualisoida ne erilleen fyysisestä puolesta. Network Virtualizationin tärkeimmät ominaisuudet ovat: verkon eristäminen ja IP-osoitteiden uudelleenkäyttö ilman VLANeja, helpompi työkuormien siirto IaaS-pilveen, reaaliaikainen migraatio eri aliverkkojen välillä, helpompi hallinta palvelinten yläpidon ja verkon ylläpidon erottamisen ansiosta, palvelinten ja verkon resurssien käytön yksinkertaistuminen ja tehostuminen, yhteensopivuus olemassa olevan infrastruktuurin kanssa ja yhteentoimivuus erilaisten konfiguraatioiden kanssa.

Verkon eristäminen ja IP-osoitteiden uudelleenkäyttö ilman VLANeja mahdollistetaan virtualisoimalla fyysinen verkko Hyper-V:n avulla ohjelmallisesti. Hyper-V huolehtii siis monikäyttäjyyden virtualisointisäännöistä ja pystyy käsittelemään paketteja, vaikka IP-osoitteet olisivat päällekkäisiä kahdessa eri virtuaalisessa aliverkossa. Esimerkiksi kahden eri yrityksen virtuaaliset tietokoneet, joilla on samat IP-osoitteet voidaan ottaa käyttöön samalla isäntäpalvelimella samoista IP-osoitteista huolimatta ja ilman VLANien avulla suoritettua verkkojen eristystä toisistaan. Koska IP-osoitteiden päällekkäisyys ei haittaa, helpottuu myös siirtyminen perinteisistä palvelinjärjestelmistä pilvijärjestelmiin, koska konfiguraatiomuutokset vähenevät eikä VLANeja tarvitse määritellä jokaiselle asiakkaalle erikseen. HNV:n avulla myös fyysisten verkkolaitteiden huolto onnistuu ilman käyttökatkoa, sillä kaikki virtuaaliset tietokoneet tietyllä isäntäpalvelimella, aliverkossa tai jopa klusterissa voidaan siirtää reaaliaikaisesti toiselle isäntäpalvelimelle ilman uudelleen konfigurointia.

Koska virtuaalisten tietokoneiden IP-osoitteet ja muut asetukset pysyvät koskemattomina, onnistuu niiden työkuormien siirto pienemmällä konfiguroinnilla mille tahansa IaaS-palveluntarjoajalle.

Tavallisesti virtuaalisten tietokoneiden työkuormien siirto reaaliaikaisesti toiselle isäntäpalvelimelle on rajoitettu samaan IP-aliverkkoon tai VLANiin, koska aliverkosta toiseen siirtyminen vaatii myös virtuaalisen tietokoneen IP-osoitteen vaihtamisen. Tämä osoitteen vaihtuminen katkaisee verkkoyhteyden ja virtuaalisella tietokoneella toimivat palvelut. HNV:n avulla reaaliaikainen työkuorman siirto kahden Windows Server 2012 palvelimen välillä onnistuu ilman IP-osoitteen vaihtamista ja näin ollen ilman käyttökatkoa. HNV pitää samalla huolen, että virtuaalisen tietokoneen sijainti ja

päivittyy ja synkronoituu kaikkien isäntäpalvelimien kanssa, joihin virtuaalinen tietokone on siirron aikana yhteydessä.

Koska HNV erottaa työkuormat eli virtuaaliset tietokoneet ja verkot toisistaan ohjelmallisesti, palvelinten ja verkon ylläpitäjät voivat keskittyä omiin tehtäviinsä välittämättä toisistaan. Palvelinten ylläpitäjät voivat esimerkiksi ottaa käyttöön uusia virtuaalisia tietokoneita tai siirtää niitä reaaliaikaisesti toiselle isäntäpalvelimelle vaihtamatta niiden IP-osoitteita tai välittämättä VLANien avulla eristetyistä verkoista.

VLANien kankeus ja virtuaalisten tietokoneiden riippuvuus fyysisestä verkkoinfrastruktuurista aiheuttaa yliprovisiointia ja resurssien käyttämättömyyttä. Rikkomalla tämän riippuvuuden, parantunut virtuaalisten tietokoneiden työkuormien sijoitus voi yksinkertaistaa verkon hallintaa ja parantaa palvelinten ja verkon resurssien käyttöä. Vaikka VLANeja käsitellään pahana asiana, on hyvä tiedostaa, että HNV tukee VLANien käyttöä fyysisen datakeskuksen tasolla eli esimerkiksi datakeskuksessa voidaan haluta kaiken HNV-liikenteen kulkevan tietyn VLANin kautta.

HNV tukee useita erilaisia konfiguraatioita kommunikointiin olemassa olevien resurssien, kuten SAN-ratkaisujen ja ei-virtualisoitujen resurssien kanssa.

HNV voidaan konfiguroida Windows PowerShellin kanssa tai käyttämällä WMI:tä eli Windows Management Intstrumentationia. Näiden hallintatyökalujen avulla voidaan konfiguroida verkon virtualisointi ja eristyssäännöt. Windows PowerShellin komentokehotteen avulla ylläpitäjät voivat luoda omia komentosarjoja automatisoidakseen konfigurointia, valvontaa tai vianrajausta varten. [57]

HNV:n toiminta

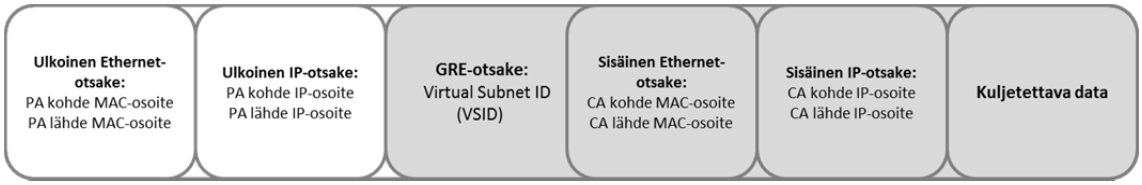
HNV:n verkon virtualisointiin käyttämä protokolla on NVGRE (Network Virtualization using Generic Routing Encapsulation), joka on samantapainen kuin VPN:ssä käytetty GRE-protokolla (Generic Routing Encapsulation). NVGRE-protokolla on erityisesti verkon virtualisointiin tarkoitettu Microsoftin, Arista Networksin, Mellanoxin, Broadcomin, Dellin, Emulexin, Intelin ja Hewlett-Packarding kehittämä protokolla [58].

NVGRE:n avulla tehty virtualisointi jakaa verkossa käytettävät IP-osoitteet kahteen kerrokseen jotka ovat PA-kerros (Provider Address) ja CA-kerros (Customer Address). PA-kerroksen osoitteet ovat tarkoitettu Hyper-V isäntäpalvelimien käytettäväksi ja se voi olla reititetty segmentti konesaliverkossa. CA-kerros on virtuaalisille tietokoneille tarkoitettu IP-osoitteisto, joka toimii virtualisoidussa verkossa. CA-kerros voi olla erillinen verkkosegmentti, jota ei ole reititetty konesalin muiden verkkosegmenttien kanssa. Esimerkiksi silloin kun CA-kerros on ulkoisen asiakkaan oma verkko, johon ulkoinen asiakas ottaa yhteyden VPN:n avulla, CA-kerrosta ei reititetä muiden konesalin verkkosegmenttien kanssa. CA-kerros voi myös olla virtualisoitava verkkosegmentti, joka reititetään konesalin muiden verkkosegmenttien kanssa tai osaksi omaa verkkoinfrastruktuuria.

HNV:n toiminta perustuu kahteen eri verkkotyyppiin VM Networkiin ja sen aliverkkoihin Virtual Subneteihin. VM Network on laajempi verkko, joka sisältää yhden tai useamman Virtual Subneteja. VM Networkit erotellaan toisistaan RDID-tunnuksilla

(Routing Domain ID) ja niiden aliverkot eli Virtual Subnetit erotellaan toisistaan VSID-tunnuksilla (Virtual Subnet ID). Tästä lähtien VM Networkista käytetään nimitystä RD ja Virtual Subnetistä nimitystä VS. RDID-tunnus määritellään datakeskuksen ylläpidon tai datakeskuksen hallintaohjelmiston toimesta. Jokainen VS kuuluu tiettyyn RD:hen ja VSID-tunnuksen tulee olla uniikki datakeskuksen sisällä. VSID-tunnus voi olla mikä tahansa kokonaisluku välillä 4096-16777214. Tämä tarkoittaa, että HNV skaalautuu hyvin isompiinkin verkkoratkaisuihin, koska VMwaren VXLANin tavoin se mahdollistaa yli 16 miljoonaa verkkoa. Samassa VSID:ssä olevat virtuaaliset tietokoneet kuuluvat samaan yleislähetys-domainiin, vastaavasti kuin VLANissa. Samassa VS:ssä olevien virtuaalisten tietokoneiden tulee käyttää samaa IP-prefiksiä eli etuliitettä, sillä jokainen VS määrittelee verkkokerroksen mukaisen IP-aliverkon. RD:n ja VS:n avulla saavutetaan yksi HVN:n tärkeimmistä asioista, sillä niiden avulla asiakkaat voivat tuoda oman aliverkkonsa pilveen. Asiakkaalle annetaan siis oma RDID, jonka alle voidaan luoda haluttu määrä virtuaalisia aliverkkoja. Kun VS luodaan hallintaohjelmistolla, järjestelmä varmaa jokaisesta osoitealueesta .1-osoitteen, jota käytetään yhdyskäytävänä eri aliverkkojen välillä. Käytännössä yhdyskäytävänä toimii HNV, eli .1-osoitteeseen kohdistettu liikenne reititetään sille. RD verkot ovat normaalisti eristetty toisistaan ja näin ne toimivat eristyksen rajoina, jolloin ei ole tarvetta VLANeille. Jos halutaan liikennöidä kahden RD:n tai RD:n ja perinteisen verkon välillä, tulee niiden välinen liikenne reitittää NVGRE Gatewayn avulla. NVGRE Gateway siis tunneloi liikenteen kahden verkon välille.

NVGRE-kapsulointia käytetään siis kahden eri sijainnissa olevan verkon yhdistämiseksi toisiinsa. NVGRE-kapsuloinnissa GRE-otsake kapsuloidaan NVGRE-paketin sisään ja lähetetään fyysistä verkkoa pitkin haluttuun etäpisteeseen. NVGRE-kapsuloitu GRE-otsake on esitelty seuraavassa kuvassa (Kuva 12).



Kuva 12: NVGRE-paketin sisältö.

NVGRE-paketti sisältää käytännössä siis GRE-otsakkeen jossa on TNI-kenttä Tenant Network Identifier) sekä sisäinen IP- ja MAC-otsake, joissa on CA-kerroksen lähde- ja kohdeosoitteet eli virtuaalisen aliverkon virtuaalisten lähde- ja kohdetietokoneiden IP-osoitteet ja MAC-osoitteet sekä kuljetettava data. TNI-kenttä sisältää virtuaalisen aliverkon tunnisteen eli VSID:n. NVGRE-paketin ulompi osa sisältää PA-kerroksen lähde- ja kohdeosoitteet eli virtuaalisen verkon Hyper-V isäntäpalvelinten lähde- ja kohdepalvelinten IP- ja MAC-osoitteet. Sisäinen GRE-otsake voi sisältää myös tiedon VLANista, jolloin reititys voidaan hoitaa myös sen avulla. Mikäli halutaan reitittää liikenne asiakkaille tai muihin verkkoihin kuin RD:stä toiseen, tulee fyysisen reitittimen tukea NVGRE-protokollaa. Tämä ei ole täysin pakollista, sillä Windows

Server 2012 R2 sisältää RAS-roolissaan NVGRE Gateway -toiminnallisuuden, jonka avulla isäntäpalvelin voidaan asettaa NVGRE yhdyskäytäväksi ja se voi liikennöidä toisen vastaavan isäntäpalvelimen kanssa. Käytännössä HNV:n käyttö vaatii siis kolme komponenttia toimiakseen: verkon virtualisointia tukevan alustan, joka Microsoftin tapauksessa on Hyper-V Extensible Switch, hallintaratkaisun, joka Microsoftin tapauksessa on System Center Virtual Machine Manager eli SCVMM ja NVGRE Gatewayn, joka on myös mahdollista toteuttaa Windows Server 2012 R2:n avulla.

NVGRE Gatewayn ominaisuudet mahdollistavat myös sen, että asiakkaalla, joka haluaa liikennöidä pilvijärjestelmässä olevien aliverkkojensa kanssa, ei välttämättä itsellään tarvitse olla NVGRE-protokollaa tukevaa laitetta. Tämä on sen ansiota, että Hyper-V -isäntäpalvelimeen asennettava NVGRE Gateway tukee myös VPN-tunnelointia. Näin ollen asiakas voi ottaa yhteyden VPN:n avulla omiin aliverkkoihinsa. [59]

4.2.4 Windows Server Gateway

Windows Server Gateway on ohjelmallisesti toteutettu virtuaaliseen tietokoneeseen asennettava reititin, joka mahdollistaa datakeskuksen ja pilveen toteutetun verkon liikennöinnin virtuaalisen ja fyysisen verkon välillä. Windows Server Gateway on myös integroitu NVGRE Gatewayhin, joka esiteltiin lyhyesti luvussa 4.2.3. Integroinnin avulla Windows Server Gatewayn eli WSG:n toiminnallisuuksia voidaan siis käyttää myös NVGRE Gatewayn kautta. WSG on ennen HNV:tä kehitetty ratkaisu, sillä ennen HNV:tä oli monimutkaista toteuttaa yhteys virtuaalisen verkon ja fyysisen verkon resurssien kuten DNS:n tai Active Directoryn välillä. WSG ratkaisi nämä ongelmat.

Tärkeimmät WSG:n toiminnallisuudet ovat: reitittää liikenne fyysisen ja virtuaalisen verkon välillä, klusterointi HA:n saavuttamiseksi, yhdyskäytävä yksityisille pilviympäristöille, site-to-site VPN hybridipilville, monikäyttäjyyttä tukeva NAT-toiminnallisuus ja monikäyttäjyyttä tukeva etäyhteys VPN:n avulla.

Yksi tärkeimmistä WSG:n tehtävistä on reitittää liikenne fyysisen ja virtuaalisen verkon välillä. Käyttötapauksia voi olla useita erilaisia kuten samassa fyysisessä sijainnissa olevan fyysisen ja virtuaalisen verkon reititys tai pilvipalvelussa sijaitsevan virtuaalisen verkon yhdistäminen omaan pilviympäristöön. Jälkimmäisessä tapauksessa yhteys muodostettaisiin VPN-yhteyden avulla.

WSG käyttöönotetaan sille dedikoidulla fyysisellä palvelinkoneella, johon on asennettu yksi virtuaalinen tietokone jossa WSG on asennettuna. Toinen vaihtoehto on klusterointi, jossa kahteen Hyper-V isäntäpalvelimeen asennetaan virtuaalinen tietokone, joista molemmat sisältävät WSG:n. Näin mahdollistetaan korkea saavutettavuus eli High Availability. Mikäli toinen isäntäpalvelimesta kaatuu, toinen toimii varayhteytenä ja toimintaa voidaan jatkaa sen kautta. Tämä onkin suositeltu tapa toteuttaa klusterointi.

WSG voi toimia myös yhdyskäytävän yksityisille pilville. Tällä tarkoitetaan esimerkiksi tilannetta, jossa yrityksellä on yhdessä fyysisessä sijainnissa oleva fyysinen verkko, joka tuottaa esimerkiksi Active Directory ja DNS-palvelut sekä virtuaalinen verkko, jossa toimivat tutkimus- ja tuotekehitysosasto sekä talousosasto. Näin ollen virtuaalisessa verkossa sijaitsevat osastot tarvitsevat fyysisen verkon palveluita. WSG voi

reitittää liikenteen virtuaalisen ja fyysisen verkon välillä ja tarjota virtuaalisessa verkossa oleville osastoille kaikki palvelut, jotka he tarvitsevat.

Hybridipilveä käyttävät ovat usein tilanteessa, jossa organisaatiolla on yksi tai useampia sivukonttoreita, jotka sijaitsevat fyysisesti eri sijainnissa. Nämä sivutoimipisteet tarvitsevat yhteyden yhteiseen datakeskukseen joka sijaitsee pilviympäristössä. Tässä tapauksessa voidaan käyttää WSG:n site-to-site VPN-yhteyttä. Sivutoimipisteillä voi olla käytössään kolmannen osapuolen tarjoama VPN-palvelin tai VPN yhdyskäytävä, jolloin he voivat käyttää sitä ottaakseen yhteyden datakeskuksessa sijaitsevaan WSG:hen ja tätä kautta pilvessä sijaitseviin yhteisiin palveluihin.

WSG tarjoaa myös perinteistä vastaavan NAT-toiminnallisuuden. Sen avulla pilviympäristössä olevat virtuaaliset tietokoneet saavat yhteyden Internetiin ilman, että jokainen tarvitsee omaa staattista IP-osoitettaan.

WSG mahdollistaa myös monikäyttäjyyttä tukevan VPN-yhteyden. Esimerkiksi sivutoimipisteistä on mahdollista ottaa tietokoneella VPN-yhteys datakeskuksen virtuaaliseen verkkoon WSG:n kautta. Monikäyttäjyydellä tarkoitetaan sitä, että datakeskuksessa voi olla useiden eri yritysten virtuaalisia verkkoja ja WSG erottelee VPN-yhteydet niin, että yritys näkee vain oman osuutensa datakeskuksen verkosta. [60]

4.3 Open vSwitch

Open vSwitch on monikerroksinen ohjelmallinen kytkin, joka on lisensoitu avoimen Apache 2 -lisenssin alla. Open vSwitchin tavoitteena on implementoida tuotantoon sopiva kytkinalusta, joka tukee standardisoituja hallintarajapintoja ja avaa eteenpäinohjauksen toiminnallisuudet ohjelmoitaviksi lisäosiksi ja hallittaviksi. Open vSwitch sopii hyvin virtuaaliseksi kytkimeksi virtualisoiduissa ympäristöissä. Sen lisäksi, että se antaa tavanomaiset hallintaominaisuudet ja näkyvyyden virtualisoituun verkkoon, se suunniteltiin myös tukemaan hajautettua toimintaa eli toimintaa useiden fyysisten palvelimien välillä. Open vSwitch tukee useita Linux-pohjaisia virtualisointiteknologioita joihin kuuluvat Citrixin XenServer, KVM ja VirtualBox. Open vSwitch on ohjelmoitu C-ohjelmointikielellä ja se on mahdollista portata eli muuntaa toimivaksi myös muissa kuin sen tukemissa isäntäpalvelimissa. [61]

Open vSwitch sijaitsee loogisesti samassa paikassa kuin esimerkiksi VMwaren vSwitch eli se asennetaan isäntäpalvelimeen. Isäntäpalvelin sisältää fyysiset verkkoadapterit ja virtuaaliset tietokoneet sisältävät virtuaaliset verkkoadapterit eli VNICit. Open vSwitch toimii siis ohjelmallisena kytkimenä isäntäpalvelimen ja virtuaalisten tietokoneiden välissä.

Avainkomponentit

Open vSwitch koostuu seuraavista komponenteista: ovs-vswitchd, ovsdb-server, ovs-dpctl, ovs-vsctl, ovs-appctl. Komponenttien nimet eivät itsessään kerro paljon toiminnasta, mutta niiden toiminta esitellään seuraavaksi. Ovs-vswitchd on daemon, jonka tarkoituksena on implementoida itse kytkin ja sen mukana Linux-kernel -moduuli vuo-

pohjaista kytkimen toimintaa varten. Daemon tarkoittaa Unix-ympäristössä taustalla suoritettavaa ohjelmaa, jota käyttäjä ei suoraan hallitse. Ovs-vswitchd on siis itse kytkin-ohjelma, joka asennetaan virtuaaliseen ympäristöön ja joka sisältää toiminnallisuuden, joka tekee siitä kytkimen. Ovsdb-server on kevyt tietokantapalvelin, jolta ovs-vswitchd eli itse kytkin pyytää tarvittavat konfiguraatiot toimiakseen. Ovs-dpctl on työkalu kytkimen kernel-moduulin eli kytkimen ytimen konfigurointia varten. Ovs-vsctl on työkalu, jonka avulla itse kytkin tekee kyselyt ja päivitykset liittyen sen konfigurointiin. Ovs-vsctl siis suorittaa tiedonvaihdon kytkimen ja tietokantapalvelimen välillä. Ovs-appctl on työkalu, joka lähettää komentoja käynnissä oleville Open vSwitch -kytkimille.

Lisäksi Open vSwitch sisältää työkaluja, joiden avulla se pystyy kommunikoimaan OpenFlowta tukevien kytkinten ja niiden hallintaohjelmien kanssa sekä tietoturvan kannalta oleellisen julkisen avaimen luontiin ja hallintaan liittyvän työkalun, jota käytetään OpenFlowta tukevien kytkinten kanssa.[61]

Ominaisuudet

Open vSwitch voidaan verrata toiminnallisuudeltaan luvussa 4.1.3 esiteltyyn dvSwitchiin. Open vSwitch tukee standardisoitua 802.1Q VLAN mallia mukaan lukien trunkingia ja access-portteja, NIC-ryhmitystä eli fyysisten verkkoadapterien ryhmittämistä sekä LACP-protokollan kanssa että ilman, NetFlowta, sFlowta ja peilausta, joilla saadaan parempi näkyvyys verkosta ja sen topologiasta, palvelun laadun konfigurointia (QoS), GRE- ja GRE-IPSEC -tunnelointia, VXLANia ja LISP-tunnelointia. Lisäksi se tukee 802.1ag-protokollaa, joka on vikojen hallintaan suunniteltu protokolla, OpenFlow 1.0 -versiota sekä useita sen lisäosia. Open vSwitch toimii käytännössä Linuxin kernel-moduulissa eli Linuxin käyttöjärjestelmän ytimessä, minkä ansiosta se tarjoaa korkean suorituskyvyn eteenpäinohjauksessa. Open vSwitchin tukee myös IPv6-protokollaa ja sen avulla on myös mahdollista määrittää liikennöintisääntöjä yhtä virtualisoitua tietokonetta kohden. [61]

Hallinta ja konfigurointi

Koska Open vSwitch on alun perin luotu C-ohjelmointikielellä, sen asentaminen ja hallinnointi tapahtuu komentokehotteen kautta. Open vSwitchin käyttö vaatii siis Unix-pohjaisen komentokehotteen hallitsemisen. Open vSwitchiin on saatavilla kuitenkin valvontaohjelma, jonka avulla pystytään valvomaan kytkimen toimintaa ja selvittämään vikatilanteita.

Open vSwitch tarjoaa siis kytkimen toiminnallisuuden ja se voidaan asentaa Citrix XenServer-, KVM- tai RedHat-isäntäpalvelimelle. Koska Open vSwitch on nimensä mukaan vapaaseen lähdekoodiin perustuva, se vaatii käyttäjältään Unixin hallintaa ja lisäksi sen toiminta perustuu paljon ohjelmistokehittäjien siihen tekemiin lisäosiin. Open vSwitch toimii myös itsenäisesti, mutta siitä saadaan mahdollisesti paras hyöty käyttämällä lisäosia. Yksi oleellinen lisäosa Open vSwitchiin on Floodlight, joka on OpenFlow-protokollaan perustuva hallintaohjelmisto. Sen toiminta perustuu SDN-

konseptiin, joka esitellään luvussa 5. Floodlightin avulla Open vSwitchiä sekä fyysisiä OpenFlowta tukevia kytkimiä voidaan hallita keskitetysti. [62]

Open vSwitchistä puuttuu ainakin toistaiseksi perinteisessä verkkoarkkitehtuurissa olevia toiminnallisuuksia kuten NAT. Open vSwitch voidaan asentaa toimimaan ainoastaan siltaavassa tilassa, eli niin, että käyttäjä määrittää itse sillatun yhteyden virtuaaliselle tietokoneelle. Periaatteessa NAT-ominaisuuden lisääminen onnistuu myös lisäosilla, mutta toistaiseksi Open vSwitch ei tue sitä. [63]

Vahvuudet

Verrattaessa Open vSwitchiä esimerkiksi VMwaren dvSwitchiin sen toiminnallisuudet ovat lähes vastaavat. VMwaren kohdalla lisäominaisuudet virtuaaliselle kytkimelle luodaan monessa tapauksessa lisätyökaluilla ja -ohjelmistoilla kuten NAT-ominaisuus luodaan vShield Edgen avulla. Jos verrataankin ainoastaan kytkinten toiminnallisuutta, ovat ne hyvin lähellä toisiaan. Lisäksi Open vSwitch tarjoaa OpenFlow-protokollan tuen, mitä ei ole VMwaren dvSwitchissä. Tämä tarkoittaa sitä, että Open vSwitch pystyy mukautumaan SDN-konseptiin paremmin kuin dvSwitch. Sitä voidaan hallita keskitetysti standardisoidun OpenFlow-protokollan avulla ja sen avulla saavutetaan lisäksi hajautetun virtuaalisen kytkimen toiminnallisuus.

Yksi tärkeimmistä asioista verkkoinfrastruktuurin suunnittelussa ja käyttöönotossa on kustannukset. Open vSwitch on ilmaisessa jakelussa oleva virtuaalinen kytkin, kun taas VMwaren dvSwitch vaatii kalleimman lisenssivaihtoehdon, Enterprise Plus -lisenssin hankkimisen. [64]

4.4 Extensible Switch, dvSwitch vai Open vSwitch?

Suurimmat kilpailijat lähiverkon virtualisoinnin kannalta ovat VMware ja Microsoft. VMwaren tuotteisiin kuuluu kaksi erilaista virtuaalista kytkintä: vSwitch ja dvSwitch. VMware erottelee nämä kaksi kytkintä toisistaan erilaisten ominaisuuksien avulla ja myös hinnalla, sillä dvSwitchin käyttö vaatii vSphere Enterprise Plus -lisenssin hankkimisen, joka on huomattavasti kalliimpi vaihtoehto kuin Windows Server 2012 R2 Hyper-V toteutuksessa heti käytettävissä oleva Extensible Switch. Huomioon kannattaa ainakin hintaan kohdistuvassa vertailussa ottaa myös Open vSwitch, joka on avoimeen lähdekoodiin perustuva ja ilmainen ratkaisu, joka voidaan toteuttaa ilmaisen KVM-hypervisorin kanssa.

Jos verrataan dvSwitchin ja Extensible Switchin toimintaa yleisesti on Extensible Switch paremmin laajennettavissa kuin dvSwitch, sillä dvSwitchiin ei ole saatavilla kolmannen osapuolen tuottamia lisäosia. DvSwitch voidaan kuitenkin vaihtaa esimerkiksi Cisco Nexus V1000 kytkimeen, joka on Ciscon kehittämä virtuaalinen kytkin. Ero laajennettavan ja suljetun kytkimen välillä ei välttämättä kuitenkaan ole niin selkeä, sillä suljettu kytkin on tavallaan suojattu kolmannen osapuolen tekemiltä laajennoksilta, jolloin sen toiminta pysyy samanlaisena kaikissa tilanteissa. Tämä saattaa helpottaa esimerkiksi vianrajausta virtuaalisessa verkossa. Tarkemmin katsottuna Extensible Swit-

chin ja dvSwitchin toiminnallisuudet ovat hyvin lähellä toisiaan ja tarjoavat hyvin monta samankaltaista ominaisuutta. Toiminnallisuuden kannalta voidaan vielä mainita pieniä eroja esimerkiksi ACL-ominaisuuden kannalta. Molemmat virtuaaliset kytkimet tukevat sitä, mutta VMwaressa tuki saavutetaan hankkimalla vCloud Suite -lisäominaisuus, mikä taas aiheuttaa lisäkustannuksia.

Skaalautuvuuden kannalta dvSwitch ja Extensible Switch ovat lähes samoissa lukemissa. Virtualisoinnin alkuvaiheessa Microsoftin tuotteet soveltuivat paremmin pienempiin pilviratkaisuihin ja VMwaren tuotteet laajempiin. Viimeisten tuotelanseerausten ja päivitettyjen järjestelmien jälkeen erot ovat kuitenkin skaalautuvuudessa pienet ja kumman tahansa valmistajan tuotteet soveltuvat niin pieniin kuin isoihinkin pilviratkaisuihin.[65]

Joitakin skaalautuvuuteen liittyviä eroja kuitenkin on, kuten porttien määrä ja maksimimäärä virtuaalisille tietokoneille isäntäpalvelimessa. Extensible Switchin tapauksessa virtuaalisten porttien määrää ei ole rajoitettu. Tämä ei kuitenkaan tarkoita rajattomuutta, sillä aktiivisten virtuaalisten tietokoneiden lukumäärä isäntäpalvelinta kohden on kuitenkin rajattu 1012 kappaleeseen. DvSwitchiin voidaan luoda 4096 virtuaalista porttia, mutta tämäkään luku ei kerro kaikkea, sillä yhteen isäntäpalvelimeen voidaan asentaa maksimissaan 512 aktiivista virtuaalista instanssia. Mikäli tutkitaan klusterikohtaisia maksimimääriä voi vSpheressä olla enintään 4000 virtuaalista instanssia ja Hyper-V:ssä 8000.

Edellä mainitut lukemat eivät kaikissa pilviratkaisuissa ole ratkaisevia tekijöitä, vaan enemmänkin toiminnallisuudet. Nämä maksimirajoitukset saavutetaan usein vain hyvin suurissa pilviympäristöissä ja pienemmissä ratkaisuissa tulevat vastaan fyysisen palvelinlaitteiston rajoitteet ennen kuin virtualisointijärjestelmien asettamat rajat.

Lopullisten kustannuserojen selvittäminen VMwaren ja Microsoftin välillä on vaikeata. Molemmat osapuolet julkaisevat omia laskelmiaan ja kertovat oman tuotteensa kustannusten olevan alhaisemmat [66]. Lopulliset kustannukset määräytyvät kuitenkin täysin halutuista ratkaisuista, joten kustannuseroja on hyvin vaikea arvioida etukäteen. Verrattaessa pienintä mahdollista ratkaisua, ovat molemmat edullisia ratkaisuja. Verkon virtualisoinnin kannalta ero tulee lähinnä siitä, että Hyper-V sisältää jokaisessa jakeluversiossaan Extensible Switchin ja verkon virtualisointiin liittyvän HNV-ominaisuuden, kun taas dvSwitchin ja VXLANin käyttö vaatii kalleimman VMwaren lisenssin. On kuitenkin tärkeätä ottaa huomioon, että verkon virtualisointi VXLANin ja HNV:n avulla hyödyttää eniten suuria verkkoinfrastruktuureja, jolloin VMwaren Enterprise Plus lisenssin hankkiminen olisi joka tapauksessa tarpeellista.[67, 68]

5 PILVIPALVELUN REDUNDANTTISUUS

Pilviympäristö on useasta eri komponentista koostuva kokonaisuus ja nopeasti kuvailtuna siitä saattaa jäädä sellainen kuva, että yhden komponentin hajotessa kaikki palvelut katoavat. Pilviympäristö on kuitenkin mahdollista luoda niin, että se on kahdennettu ja sen toimintavarmuus on korkealla. Koska pilvipalvelu on suurelta osaltaan virtualisoitu ympäristö, pitää kahdennuksen olla toteutettuna myös siihen liittyvissä fyysisissä verkkolaitteissa. Tämä on syy miksi pilven infrastruktuuri koostuu hyvin usein esimerkiksi kahdesta ESXi-isäntäpalvelimesta ja useasta fyysisestä verkkoadapterista. VMwaren infrastruktuurissa kahdennus ja toimintavarmuus pidetään yllä näiden lisäksi myös ohjelmallisilla toteutuksilla, jotka ovat virtualisoidun ympäristön puolella. Näitä ovat esimerkiksi VMwaren VMotion, HA ja FT (Fault Tolerance) ja Microsoftin LBFO. Tässä luvussa käsitellään VMwaren VMotionin, HA:n ja FT:n toiminta, koska niitä käytettiin verkon redundanttisuuden testaamiseen pilvijärjestelmässä.

5.1 Reaaliaikainen migraatio

VMotion on VMwaren pilvi-infrastruktuurin lisäominaisuus, joka mahdollistaa reaaliaikaiseen virtuaalisten tietokoneiden migraation fyysiseltä ESXi-isäntäpalvelimelta toiselle. Reaaliaikaisuudella tarkoitetaan sitä, että virtuaalista palvelinta ei tarvitse sammuttaa siirron ajaksi ja sen tuottamat palvelut, kuten verkkokauppa, pysyvät toiminnassa ilman minkäänlaista käyttökatkoa. VMotion mahdollistaa siis dynaamisen, automatisoidun ja itsestään optimoituvan datakeskuksen luomisen. Reaaliaikaisesta migraatiosta on hyötyä myös ylläpitäjien kannalta, sillä se mahdollistaa fyysisen laitteiston huoltojen tekemisen ilman palvelun katkaisua, sen avulla voidaan siirtää virtuaalisia tietokoneita muualle jo ennen kuin vikatilanne sattuu ja sen avulla voidaan optimoida pilviympäristön toimintaa siirtämällä virtuaalisia tietokoneita vähemmän kuormitetuille ESXi-isäntäpalvelimille.

VMotionin toiminnan mahdollista kolme teknologiaa. Ensimmäiseksi koko virtuaalisen tietokoneen tila ja tiedot kapsuloidaan tiedostoihin, jotka sijaitsevat jaetussa levyjärjestelmässä kuten iSCSI-SAN, Fibre Channel tai NAS. VMwaren vStorage VMFS-tiedostojärjestelmä mahdollistaa usean ESXi-isäntäpalvelimen pääsyn samoihin virtuaalisen tietokoneen tiedostoihin samanaikaisesti. Samanaikainen pääsy tiedostoihin varmistaa siis sen, että uusi ESXi-isäntäpalvelin, johon virtuaalinen tietokone siirretään, saa välittömästi kaikki sen tarvitsemat tiedot, jotta se voi käynnistää vastaavan virtuaalisen tietokoneen välittömästi.

Toinen tärkeä teknologia on virtuaalisen tietokoneen aktiivisen muistin ja täsmällisen suoritustilan siirtäminen uudelle ESXi-isäntäpalvelimelle nopean verkon kautta. Tämä mahdollistaa virtuaalisen tietokoneen ylläpitämän palvelun jatkumisen täsmäl-

leen siitä hetkestä, johon se jäi ollessaan vanhassa ESXi-isäntäpalvelimessa. VMotion pitää siirtoon kuluvan ajan huomaamattomana käyttäjille pitämällä kirjaa juuri tapahtuvista muistitapahtumista bittikartassa. Kun virtuaalisen tietokoneen koko muisti ja tila on siirretty uudelle ESXi-isäntäpalvelimelle VMotion pysäyttää lähteenä toimineen virtuaalisen tietokoneen, kopioi muistikartan uudelle ESXi-isäntäpalvelimelle ja palauttaa virtuaalisen tietokoneen toiminnan samaan hetkeen johon se jäi vanhalla ESXi-isäntäpalvelimella. Tämä koko prosessi tapahtuu alle kahdessa sekunnissa, mikäli käytössä on Gigabit-nopeudella toimiva lähiverkko.

Kolmantena on verkon toiminnasta huolehtiminen. Virtuaalisen tietokoneen verkkotiedot säilytetään myös ESXi-isäntäpalvelimella. Tämä mahdollistaa verkon toiminnan jatkumisen vaikka virtuaalinen tietokone siirtyy eri ESXi-isäntäpalvelimelle ja samalla myös uudelle fyysiselle verkkokortille. VMotion hallitsee myös virtuaalisia MAC-osoitteita osana prosessia. Kun siirtoprosessi uudelle ESXi-isäntäpalvelimelle on suoritettu kaiken muun osalta ja virtuaalinen tietokone uudelleenkäynnistetty uudessa alustassaan VMotion ilmoittaa verkon reitittimille asiasta varmistaen, että reititin on tietoinen virtuaalisen MAC-osoitteen uudesta fyysisestä verkkosijainnista. Koska virtuaalisen tietokoneen migraatio VMotionilla säilyttää täsmällisen suoritustilan, verkkotiedot ja aktiiviset verkkoyhteydet, tuloksena ei synny lainkaan katkoa verkkoyhteyteen tai palvelun käyttäjiin. [69]

VMotionin kanssa suositellaan käytettäväksi sille dedikoitua Gigabit-Ethernet tiedonsiirtoväylää. Tämä tarkoittaa sitä, että esimerkiksi kahden ESXi-isäntäpalvelimen tapauksessa klusterissa on käytössä yhteensä neljä fyysistä verkkoadapteria. Jotta VMotionin suosittelema vaatimus tulisi täytettyä, tulisi käyttöön ottaa vielä yksi fyysinen verkkoadapteri molempia ESXi-isäntäpalvelinta kohden. Mikäli ei ole mahdollista käyttää VMotionille dedikoitua väylää, tulisi parhaan tietoturvan saavuttamiseksi dedikoida toinen fyysisistä verkkoadaptereista VMotionin käyttöön ja jakaa toinen verkkoadapteri VLANien avulla virtuaalisten tietokoneiden liikenteelle ja hallinnan liikenteelle. Parhaan saatavuuden takaamiseksi taas tulisi molemmat fyysiset verkkoadapterit ryhmittää yhteen ja käyttää VLANeja liikenteen jakamiseen VMotionille, virtuaalisten tietokoneiden liikenteelle ja hallinnan liikenteelle. [70]

5.2 High Availability

High Availability eli HA on lisäominaisuus, jonka tarkoitus on taata virtuaalisten palvelimien tarjoamien palveluiden ja sovellusten saatavuus vikatilanteissa. HA:n avulla voidaan minimoida huoltokatkojen aiheuttamien palvelukatkojen pituudet ja poistaa tarve dedikoitujen fyysisten varalaitteiden ylläpitämiselle. Käytännössä HA toimii niin, että virtuaalisen tietokoneen sisältävän fyysisen ESXi-isäntäpalvelimen vikaantuessa kyseessä oleva virtuaalinen tietokone siirretään toiselle ESXi-isäntäpalvelimelle ja käynnistetään siellä uudestaan. Mikäli ESXi-isäntäpalvelin ei vikaannu, mutta itse virtuaalisen tietokoneen käyttöjärjestelmän toiminta pysähtyy, käynnistää HA-ominaisuus virtuaalisen tietokoneen uudelleen samassa ESXi-isäntäpalvelimessa.

HA:n tarkoitus on suojata palveluita ja sovelluksia, joilla ei ole muita failover-vaihtoehtoja. Korkean saatavuuden ratkaisut ovat usein monimutkaisia, kalliita ja ne ovat usein käytössä vain kriittisissä sovelluksissa. HA:n tavoite onkin saavuttaa kustannustehokas tapa varmistaa saatavuus myös muille sovelluksille ja palveluille, jotka eivät kuulu kriittisiin sovelluksiin. Usein korkean saatavuuden ratkaisut ovat lisäksi sidottuja tiettyyn käyttöjärjestelmään tai sovelluksiin ja ovat tämänkin vuoksi monimutkaisia käyttää. HA:ta voidaankin käyttää kaikkien järjestelmien ja sovellusten kanssa, sillä se ei vaadi niiltä erikseen tukea toimiakseen.

HA toimii valvomalla jatkuvasti kaikkia haluttuja virtuaalisia palvelimia ja tunnistaa fyysisen ESXi-isäntäpalvelimen ja käyttöjärjestelmän vikaantumisen. ESXi-isäntäpalvelinten valvontaa varten se käyttää fyysiselle palvelinkoneelle asennettua agenttia, joka ylläpitää tietynlaista jatkuvaa kommunikointia muiden klusterissa olevien fyysisten palvelinten kanssa. VMware kutsuu tätä jatkuvaa kommunikointia nimellä heartbeat eli sydämen syke. Kun jatkuva kommunikointi syystä tai toisesta katkeaa, käynnistää HA virtuaaliset tietokoneet toisella ESXi-isäntäpalvelimella.

HA käyttää hyväkseen jaettua levytilajärjestelmää samalla tavalla kuin VMotion. Tämä mahdollistaa muiden ESXi-isäntäpalvelinten pääsyn samalle levyjärjestelmälle ja näin ollen virtuaalisen tietokoneen tiedostojen käytön. HA ei kopioi uudelle ESXi-isäntäpalvelimelle kuitenkaan virtuaalisen tietokoneen täsmällistä suoritustilaa tai aktiivista muistia, joten kun virtuaalinen tietokone käynnistetään uudella ESXi-isäntäpalvelimella, se käynnistyy alusta asti.

Valvoakseen käyttöjärjestelmien vikaantumista HA käyttää jokaiselle virtuaaliselle tietokoneelle asennettua sydämen syke-toimintoa hyväkseen. Vika huomataan tällöin siinä tapauksessa kun virtuaalinen tietokone ei ilmoita toiminnastaan käyttäjän määrittämään määräaikaan mennessä. VMware HA huolehtii myös siitä, että klusterissa jossa se toimii, on riittävästi resursseja käynnistää uudelleen HA-ominaisuuden alaisuuteen kuuluvat virtuaaliset tietokoneet.

Käytännössä HA määritellään toimimaan tietyssä resource poolissa eli resurssialtaassa. Tämä tarkoittaa sitä, että kaikki tähän samaan resurssialtaaseen kuuluvat virtuaaliset tietokoneet kuuluvat HA:n alaisuuteen. Resurssialtaalla tarkoitetaan tiettyä osaa virtuaalisesta ympäristöstä, johon kuuluu tietty osa fyysisten ESXi-isäntäpalvelinten resursseista, levytilajärjestelmien resursseista ja verkkoresursseista. [71]

HA on yleisesti ajatellen monimutkaisia ja kalliita saatavuuden vaihtoehtoja helpompi ratkaisu, mutta kriittisiin sovelluksiin se ei sovi juuri sen takia, että uudelleenkäynnistykseen kuluu tietty aika vikatilanteen sattuessa. Vaikka tämä aika ei käytännössä ole pitkä, saattavat jotkin toiminnallisuudet vaatia jatkuvan toimivuuden, jolloin seuraavaksi esiteltävä Fault Tolerance eli FT on parempi vaihtoehto.

5.3 Fault Tolerance

VMwaren Fault Tolerance eli FT on lisäominaisuus, jonka tavoitteena on HA:n tavoin varmistaa saatavuus virtuaalisten tietokoneiden palveluille ja sovelluksille. Se eroaa HA:sta kuitenkin siinä, että saatavuus on jatkuvaa. Tällä tarkoitetaan sitä, että vikatilanteen sattuessa joko fyysisessä ESXi-isäntäpalvelimessa tai virtuaalisen tietokoneen käyttöjärjestelmässä, loppukäyttäjä ei huomaa lainkaan sitä, vaan virtuaalinen palvelin siirtyy toiselle ESXi-isäntäpalvelimelle ilman käyttökatkoa. Ilman käyttökatkoa vältytään samalla myös tietojen menettämiseltä. Vaikka FT on HA:n tavoin riippumaton käyttöjärjestelmästä, on otettava huomioon, että FT tukee ainoastaan yhdellä virtuaalisella prosessorilla konfiguroituja virtuaalisia tietokoneita. Tämä saattaakin olla ongelma sillä esimerkiksi paljon kuormitetut sähköpostipalvelimet tai tietokantapalvelimet saattavat vaatia useamman virtuaalisen prosessorin käytön toimiakseen tehokkaasti. Tällöin ainoa vaihtoehto VMwaren toiminnallisuuksista on käyttää HA-ominaisuutta. VMware on ilmoittanut suunnittelevansa ratkaisua, jolloin yhden virtuaalisen prosessorin rajoite saataisiin poistettua, mutta tarkempaa tietoa asiasta ei ole annettu [72].

Kun VMware FT asetetaan aktiiviseksi virtuaalisessa tietokoneessa, se luo reaaliaikaisen kopion käynnissä olevasta virtuaalisesta tietokoneesta, joka pidetään käynnissä toisella ESXi-isäntäpalvelimella. Alkuperäinen virtuaalinen tietokone ja sen kopio pidetään virtuaalisesti samalla tasolla jatkuvasta VMwaren vLockstep-teknologian avulla. vLockstep kirjaa ylös kaikki alkuperäisen virtuaalisen tietokoneen tekemät suoritteet ja lähettää ne Gigabit-nopeuksisen lähiverkon kautta kopiona toimivalle virtuaaliselle tietokoneelle, joka toistaa suoritteet samalla tavalla kuin alkuperäinen. Nämä kaksi virtuaalista tietokonetta suorittavat siis täysin samat käskyt millä tahansa hetkellä, koska niiden syötteet ovat täysin samat. Sekä alkuperäisellä että kopiona toimivalla virtuaalisella tietokoneella on pääsy yhteiselle levytilalle ja muille sovelluksille ne näyttävät olevan yksi ainoa kokonaisuus, jolla on yksi IP-osoite ja MAC-osoite. Ainoa ero alkuperäisen virtuaalisen tietokoneen ja kopion välillä on, että ainoastaan alkuperäisellä virtuaalisella tietokoneella on kirjoitusoikeus. Nämä kaksi virtuaalista tietokonetta kommunikoivat keskenään heartbeatin avulla. FT:n tapauksessa heartbeat eli sydämen syke toiminto tapahtuu millisekunnin välein. Mikäli toinen virtuaalisista tietokoneista ei vastaa kommunikointiin, ottaa toinen instanssi välittömästi alkuperäisenä toimivan virtuaalisen tietokoneen aseman. Määräajan ollessa näin lyhyt ei myöskään ehdi syntyä minkäänlaista datan menetystä toisen virtuaalisen tietokoneen jatkaessa toimintaa.

FT toimii siis periaatteellisesti hieman samalla kuin VMotion. On kuitenkin tärkeä huomioida, että nämä ovat kaksi täysin erillistä ominaisuutta, joten molempien ollessa käytössä, tulee myös molemmilla olla omat dedikoidut tiedonsiirtoväylät. [73]

FT:n käyttöönotossa on tärkeää ottaa huomioon oman pilviympäristön resurssit. Koska FT pitää käynnissä samanaikaisesti kahta virtuaalisen tietokoneen instanssia, tulee myös resurssien, kuten laskentatehon ja muistin olla kaksinkertainen. Levytilan kannalta käyttöönotossa ei ole merkitystä, sillä ne käyttävät yhteistä levytilaa. Vaikka VMware kertoo FT:n olevan edullinen ja yksinkertainen tapa luoda jatkuva saatavuus

palveluille, tulee kustannuksia joka tapauksessa laskentatehon ja muistin lisäämisestä järjestelmään. Jos pilviympäristössä halutaan käyttää FT-ominaisuutta, tulee suunnitteluvaiheessa ottaa tarvittavat resurssit tarkasti huomioon.

5.4 Verkon redundanttisuuden testaaminen

Lähiverkon redundanttisuuden testaaminen toteutettiin VMwaren pilviympäristössä käyttämällä ping-työkalua. Virtuaaliseen testikoneeseen asetettiin vuorotellen päälle HA- ja FT-ominaisuudet. Testin tarkoituksena oli selvittää kuinka pitkä palautumisaika on vikatilanteesta, kun käytössä on HA-ominaisuus ja FT-ominaisuuden kanssa haluttiin todentaa verkkoyhteyden katkeamattomuus. Vikatilannetta simuloitiin käynnistämällä klusterin virtuaalista tietokonetta isännöivä ESXi-isäntäpalvelin uudelleen, jolloin sekä HA:n ja FT:n tulisi siirtää virtuaalisen tietokoneen toiminta toiselle ESXi-isäntäpalvelimelle.

Ping-työkalua käytettiin niin, että HA:n tapauksessa sisäverkossa olevalla hallintakoneella pingattiin virtuaalista tietokonetta, jonka ESXi-isäntäpalvelin joutuu vikatilaan ja toiminta siirtyy toiselle laitteelle. FT:n tapauksessa pingaus suoritettiin sekä virtuaaliselta tietokoneelta verkon hallintakoneelle kuin myös toiselta virtuaaliselta tietokoneelta vikaantuvalle virtuaaliselle tietokoneelle. Ping-pakettien lähettäminen aloitettiin tietysti molemmissa tapauksissa ennen simuloidun vikatilanteen alkamista.

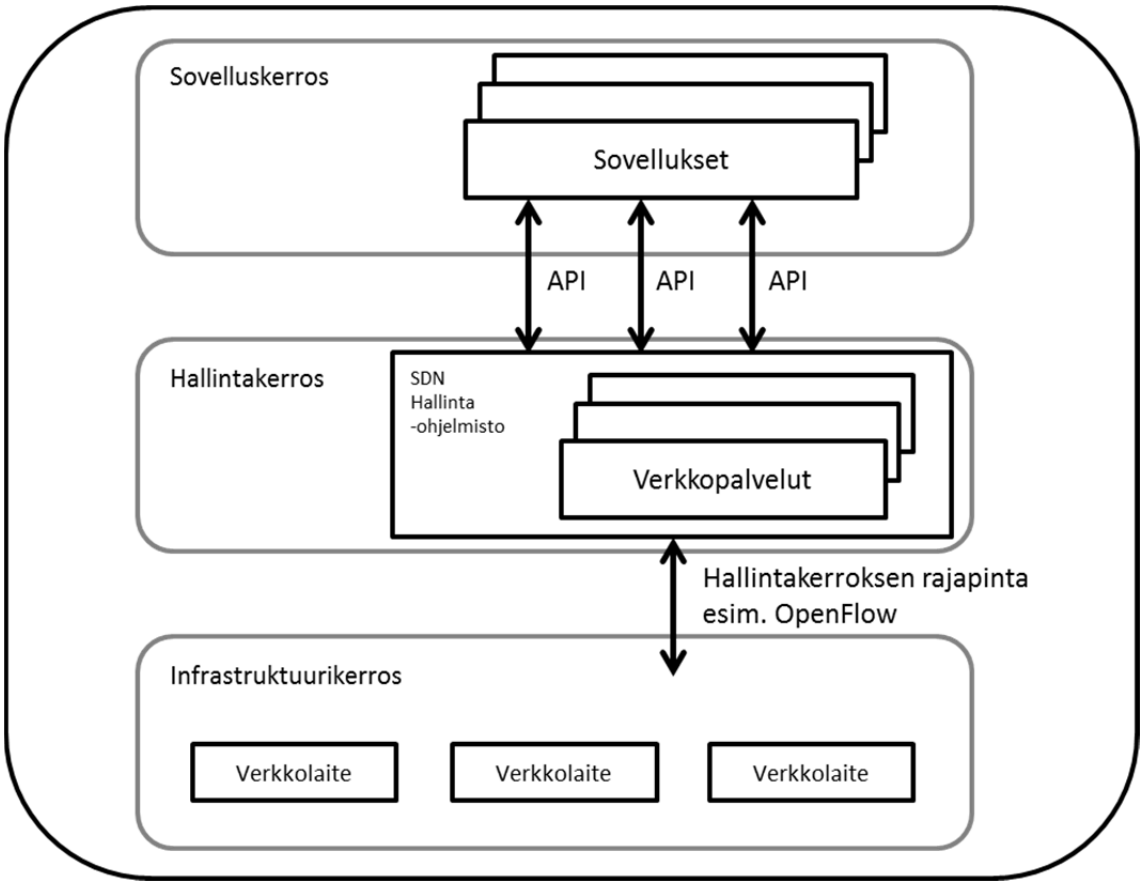
HA-ominaisuuden todettiin toimivan niin kuin sen on luvattukin. Tuloksista nähtiin selkeästi, että yhteys katkeaa alkuperäisessä ESXi-isäntäpalvelimessa olevaan virtuaaliseen tietokoneeseen ja ping-paketteja häviää noin 60 kappaletta katkon aikana. Tämän jälkeen yhteys palautuu normaaliksi ja myös viiveet normalisoituvat. Ping-työkalu lähettää oletuksena yhden paketin sekunnin aikana, joten 60 vastaamattoman paketin avulla voidaan sanoa yhteyden olleen katki noin 60 sekunnin ajan. Tähän aikaan kuuluvat HA-ominaisuuden kannalta siis vikatilanteen tunnistus, virtuaalisen tietokoneen käynnistäminen vaihtoehtoisessa ESXi-isäntälaitteessa ja verkkoyhteyden tietojen ilmoittaminen verkon fyysiselle kytkimelle, joten 60 sekunnin ajan voidaan ajatella olevan suhteellisen lyhyt.

Jotkin kriittiset sovellukset ja palvelut vaativat jatkuvan toimivuuden, joten testasimme verkon redundanttisuuden myös FT:n tapauksessa, jolloin loppukäyttäjän ei pitäisi huomata minkäänlaista käyttökatkoa vikatilanteen syntyessä ja siitä toipumisessa. Lähetimme FT:n tapauksessa siis ping-paketteja molempiin suuntiin, jolloin saimme varman kuvan yhteyden katkeamattomuudesta. Tuloksista voitiin todeta, että lähetettäessä ICMP-paketteja FT-suojattuun virtuaaliseen tietokoneeseen, on vaikea havaita edes vikatilanteen alkuhetkeä. Koska vikatilanne oli simuloitu, tiedetään vikatilanteen kuitenkin tapahtuneen noin 45 sekunnin jälkeen ping-työkalun käytön aloittamisesta, jolloin viive kasvoi noin 8 millisekuntiin yhden paketin ajaksi. FT-suojatulta koneelta ulospäin pingattaessa viive kasvoi noin 14 millisekuntiin. FT-suojauksen voidaankin tämän testin perusteella toimivan odotetusti ja molemmista suunnista tehty ICMP-

pakettien lähettäminen todentaa, että yhtään pakettihäviötä ei kumpaankaan suuntaan syntynyt ja yhteys ei näin ollen katkennut hetkeksikään.

6 SDN – SOFTWARE-DEFINED NETWORKING

Software-defined networking (SDN) eli ohjelmallisesti määritelty verkko on konsepti, jonka tavoite on yksinkertaistaa verkkojen luomista ja hallintaa. SDN:n päätavoitteena on erotella perinteisessä tietoliikenneverkossa oleva dataa liikuttava osa (data plane) ja itse reitityksestä sekä verkkoliikenteen ohjauksesta päättävä osa (control plane) toisistaan. Tässä luvussa tutustutaan SDN-konseptin ideaan ja toteutukseen sen teorian kannalta. SDN on Open Networking Foundationin (ONF) eteenpäin ajama ja OpenFlow-standardiin perustuva konsepti. SDN:n arkkitehtuuri ja looginen toiminta esitellään kuvassa (Kuva 12).



Kuva 13: SDN-arkkitehtuuri ja looginen toiminta. [74]

Kuvassa (Kuva 12) on selkeä looginen esittely SDN:stä. Perinteisessä verkkoarkkitehtuurissa hallintakerros ja infrastruktuurikerros ovat yhdessä ja SDN erottaa ne toisistaan. Käytännössä tämä tarkoittaa sitä, että verkkolaitteiden eteenpäinohjauksesta päättävät toiminnallisuudet ohitetaan ja niitä hallitaan SDN:n hallintaohjelmiston avulla.

Esimerkiksi kytkimissä tämä on toteutettu niin, että laitevalmistajat sallivat kytkimen hallinnan OpenFlown avulla eli kytkin sallii SDN-hallintaohjelmiston hallita kytkimen toimintaa oman kytkimen sisäänrakennetun ohjelmiston ohi. OpenFlow onkin äärimmäisen tärkeä osa SDN-konseptia ja sen toimintaperiaatteet esitellään luvussa 5.2.1.

Sen lisäksi, että fyysinen verkkoinfrastruktuuri abstrahoidaan hallintakerroksesta, SDN-arkkitehtuuri tukee joukkoa API-rajapintoja (Application Programming Interface). APIt toimivat SDN-hallintaohjelmiston ja sovellusten välissä. APIen avulla voidaan määritellä miten tietyt ohjelmistokomponentit keskustelevat toistensa kanssa. APIen avulla SDN-arkkitehtuuriin voidaan implementoida yleisimpiä verkkopalveluita kuten reititys, ryhmälähetys, tietoturva, pääsynhallinta, kaistanleveyden hallinta, liikenteen muokkaus, palvelun laatu (QoS), prosessori ja levytilajärjestelmien optimointi, virrankäyttö ja erilaisten sääntöjen hallinta juuri tietynlaisia organisaation vaatimuksia varten. Esimerkiksi SDN-arkkitehtuuri mahdollistaa APIen avulla johdonmukaiset säännöt niin langallisille kuin myös langattomille yhteyksille kampusalueella. [74]

6.1 Miksi SDN?

Mobiililaitteiden määrän ja sisällön valtava kasvu, palvelinvirtualisointi ja pilvipalvelut ovat trendejä, jotka ovat pakottaneet tietoliikennealan tutkimaan vaihtoehtoja perinteisille verkkoratkaisuille. Monet perinteiset verkot ovat hierarkkisesti toteutettuja eli ne ovat koostuvat kerroksista Ethernet-kytkimiä, jotka muodostavat puumaisen rakenteen. Tämä malli oli hyvä kun suurin osa yhteyksistä perustui asiakas-palvelin -malliin, mutta nykyiseen dynaamiseen laskentaresurssien ja levytilajärjestelmien käyttöön niin palveluntarjoajilla, kampuksilla kuin datakeskuksissa, se ei ole enää riittävän joustava.

Markkinoiden luomia vaatimuksia ei ole mahdollista enää toteuttaa tehokkaasti nykyisellä verkkoarkkitehtuurilla. Yritysten IT-osastot joutuvat jatkuvasti pärjäämään pienemmällä budjetilla ja yrittävät saada kaiken irti vanhemmista laitteistaan yksittäisten laitteiden hallintatyökaluilla ja käsin tehtävillä prosesseilla. Palveluntarjoajat kärsivät vastaavanlaisista ongelmista kun kysyntä liikkuvuudelle ja kaistanleveydelle kasvaa jatkuvasti. Liikevoitot menevät laitteiden jatkuvasti kasvaviin kustannuksiin ja joko tasaiseen tai tulosta vähentävään liikevaihtoon. Nykyistä verkkoarkkitehtuuria ei ole suunnittelu nykypäivän tarpeisiin ja monet joutuvat tyytymään sen asettamiin rajoituksiin. Seuraavissa kappaleissa esitellään suurimpia nykyisessä verkkoarkkitehtuurissa olevia ongelmia. [74]

6.1.1 Monimutkaisuuden aiheuttama staattisuus

Tähän päivään asti verkkoteknologia on koostunut suureksi osaksi diskreeteistä protokollista, jotka on suunniteltu yhdistämään laitteita toisiinsa luotettavasti, satunnaisten välimatkojen, nopeuksien ja topologioiden kautta. Vastatakseen kasvaviin liiketoiminnallisiin ja teknisiin vaatimuksiin, on alalla kehitetty erilaisia protokollia, joilla voidaan saavuttaa parempi suorituskyky, luotettavuus, laajempi yhdistettävyys ja tiukempi tietoturvallisuus. Yleisesti protokollilla on taipumus olla eristetysti määriteltyjä eli ne ovat

ratkaisu tiettyyn ongelmaan ratkaisematta suurempaa tarkoitusta. Tästä on seurannut yksi nykyisen verkkoarkkitehtuurin ongelmista, monimutkaisuus. Esimerkiksi lisätäkseen tai siirtääkseen verkkolaitteen ylläpitäjän tulee käsitellä useita kytkimiä, reitittimiä, palomuureja, autentikointiportaaleja, päivittää VLAN-tiedot, huolehtia QoS:sta ja muista protokollapohjaisista mekanismeista käyttäen laitekohtaisia hallintatyökaluja. Tämän lisäksi verkon topologia, laitevalmistajan kytkimen malli ja ohjelmistoversio tulee ottaa huomioon. Tämän monimutkaisuuden vuoksi nykypäivän verkot ovat suhteellisen staattisia kun pyritään minimoimaan palvelukatkojen riskit.

Nykyisten verkkojen staattisuus on suhteessa hyvin suuri verrattuna nykyiseen palvelinympäristöjen dynaamisuuteen, missä suureksi osaksi on siirrytty palvelinvirtualisointiin. Palvelinvirtualisointi on huomattavasti kasvattanut liikennöivien laitteiden määrää ja samalla muuttanut oletuksen siitä missä ne fyysisesti sijaitsevat. Ennen virtualisointia sovellukset olivat yhdellä palvelimella ja pääasiassa ne liikennöivät vain tiettyjen asiakkaiden kanssa. Nyt sovellukset on jaettu useille virtuaalisille tietokoneille, jotka käsittelevät liikennettä keskenään. Virtuaaliset tietokoneet siirtyvät palvelimelta toiselle optimoinnin takia ja tasapainottavat palvelimien kuormaa aiheuttaen samalla fyysisten liikenteen päätepisteiden vaihtumisen välillä jopa hyvin nopealla aikavälillä. Virtuaalisten tietokoneiden migraatio asettaa haasteita perinteiselle verkkoarkkitehtuurille esimerkiksi reitityksen ja segmentoinnin kannalta.

Kasvaneen virtualisoinnin lisäksi useat yritykset käyttävät nykyään IP-verkkoa siirtääkseen ääni-, data- ja videoliikennettä. Nykyiset verkot pystyvät tarjoamaan QoS-palvelua näille toiminnoille, mutta niiden käyttäminen on hyvin paljon käsin tehtävää konfigurointia. Ylläpidon tulee konfiguroida jokaisen laitevalmistajan laitteet erikseen ja määrittää niihin parametrit kuten kaistanleveys ja QoS istuntoa sekä sovellusta kohden. Tämän staattisuuden vuoksi verkko ei pysty dynaamisesti sopeutumaan muuttuvaan liikenteeseen eikä sovellusten tai käyttäjän vaatimuksiin. [74]

6.1.2 Epäjohdonmukaiset säännöt

Implementoidakseen perinteiseen verkkoarkkitehtuuriin koko verkkoa koskevan säännön ylläpito joutuu konfiguroimaan mahdollisesti jopa tuhansia verkkolaitteita ja mekanismeja. Esimerkiksi kun uusi virtuaalinen tietokone tuodaan verkkoon voi kestää useita tunteja tai jopa päiviä, jotta ylläpito saa uudelleenkonfiguroitua pääsynhallintasäännöt koko verkon alueelta. Nykyisen verkkoarkkitehtuurin monimutkaisuus tekee ylläpidolle hyvin vaikeaksi määritellä johdonmukainen pääsyn, tietoturvan, QoS:n ja muiden sääntöjen joukko jatkuvasti liikkuville käyttäjille. Tämän vuoksi yrityksen tietoturva saattaa vaarantua tai esimerkiksi määräysten noudattaminen tulee vaikeaksi. [74]

6.1.3 Skaalautumattomuus

Datakeskusten vaatimusten kasvaessa kasvavat myös verkon vaatimukset. Nykyisessä tilassa verkosta tulee kuitenkin hyvin monimutkainen, kun siihen lisätään tuhansia verkkolaitteita, jotka kaikki pitää konfiguroida ja tämän jälkeen hallita. Lisäksi verkossa

usein luotetaan linkkien ylikuormittamiseen eli siihen, että yhdelle linkille asetetaan mahdollista liikennettä enemmän kuin se pystyisi tehokkaasti käsittelemään. Tämä perustuu liikenteen valvontaan ja siihen, että kaikki laitteet eivät käytä koko kaistanleveyttä jatkuvasti. Nykyisissä virtualisoiduissa ympäristöissä verkkoliikenne on kuitenkin hyvin dynaamista, mikä tekee hyvin vaikeaksi arvioida liikenteen määrää esimerkiksi vuorokauden tai ajan mukaan.

Skaalautuvuuden kanssa vielä suurempiin vaikeuksiin joutuvat hyvin suuret operaattorit kuten Google, Yahoo! ja Facebook. Nämä palveluntarjoajat käyttävät laajaalaisia rinnakkaisia prosessointialgoritmeja ja yhteistyössä toimiva datakeskuksia koko resurssialtaansa alueella. Esimerkiksi loppukäyttäjän hakiessa jotakin asiaa, sovellus etsii ja indeksoi koko Internetin alueelta dataa palauttaakseen loppukäyttäjälle tiedon mahdollisimman nopeasti. Tällöin tiedonsiirto ja laskentaelementtien määrä kasvaa erittäin suureksi ja laskentasolmujen välillä saattaa liikkua jopa petatavujen verran liikennettä. Nämä suuret operaattorit tarvitsevatkin käyttöönsä niin sanottuja hyperskaalautuvia verkkoja, jotka tarjoavat korkean suorituskyvyn ja edullisen tavan yhdistää palvelimia jopa sadoista miljooniin. Tällaista skaalautuvuutta ei ole mahdollista saavuttaa perinteisellä verkkoarkkitehtuurilla ja käsin tehtävällä konfiguroinnilla.

Pysyäkseen kilpailukykyisinä palveluntarjoajien on tarjottava asiakkailleen aina vain parempaa arvoa ja laatua sekä hyvällä tavalla paremmin erottuvia palveluita. Monikäyttäjyys aiheuttaa palveluntarjoajille haasteita, sillä verkon tulisi palvella asiakkaiden ryhmiä, jotka käyttävät erilaisia sovelluksia ja joilla on erilaiset suorituskykyvaatimukset. Tärkeät toiminnallisuudet, jotka vaikuttavat hyvin yksinkertaisilta, ovat hyvin monimutkaisia implementoida olemassa olevilla verkoilla, varsinkin kun puhutaan palveluntarjoajien käsittelemistä verkon kokoluokista. Esimerkkinä tärkeästä toiminnallisuudesta voisi olla asiakkaiden liikenteen ohjaaminen, jotta voidaan tarjota muokattua suorituskyvyn hallintaa tai on-demand toimitusta. Nämä toimenpiteet vaativat erikoislaitteita verkon reunalle ja tämä tarkoittaa taas investointien kasvua ja toiminnasta aiheutuvia kustannuksia kuten myös ajankäyttöä. [74]

6.1.4 Riippuvuus laitevalmistajasta

Palveluntarjoajat ja yritykset etsivät jatkuvasti uusia tapoja ottaa käyttöön uusia toiminnallisuuksia vastatakseen liiketoiminnan ja käyttäjien tarpeisiin. Kyky uusien toiminnallisuuksien käyttöönottoon kuitenkin heikentyy laitevalmistajien laitteiden tuotantosyklien takia. Nämä tuotantosyklit saattavat vaihdella vuodesta kolmeen vuoteen tai vielä pidempään. Standardien mukaisten avointen liityntöjen puute rajoittaa verkkooperaattoreita muokkaamasta verkkoa omiin tarpeisiinsa sopiviksi.

Nämä sopimattomuudet markkinoiden vaatimusten ja verkkojen antamien mahdollisuuksien välillä ovat olleet merkittävä tekijä SDN:n tarpeellisuudessa. Näiden asioiden vuoksi Open Network Foundation on kehittänyt SDN-arkkitehtuurin ja kehittää samalla siihen liittyviä standardeja. [74]

6.2 OpenFlow

OpenFlow on ensimmäinen standardi liikennöintirajapinta, joka on määritelty hallintakerroksen ja datakerroksen välille SDN-arkkitehtuurissa. OpenFlow sallii suoran pääsyn ja manipuloinnin sekä fyysisten että virtuaalisten kytkinten ja reitittimien eteenpäinohjaustoiminnallisuuteen. Yksi syy nykyisten verkkolaitteiden olemiseen laitevalmistajakohtaisia ja suljettuja on se, että ei ole ollut olemassa yhtä standardia, jolla kaikkia voitaisiin ohjata. OpenFlow onkin ainoa laatuaan ja ilman sitä ei ole mahdollista siirtää verkkolaitteiden hallintaa keskitetyksi, ohjelmistolla suoritettavaksi toiminnoksi.

OpenFlowta voidaan verrata prosessorien käskykantoihin. Se määrittelee peruskäskyt, joita ulkoiset sovellukset voivat käyttää ohjelmoidakseen verkkolaitteiden toiminnan haluamakseen, aivan kuten prosessorien käskykannoilla ohjelmoitaisiin tietokonejärjestelmä.

OpenFlow-protokolla implementoidaan molemmille puolille rajapintaa eli sekä SDN-hallintaohjelmiston puolelle että verkkoinfrastruktuurin verkkolaitteiden puolelle. OpenFlow käyttää liikenteen tunnistamiseen valmiiksi määritettyjä sääntöjä, jotka voidaan staattisesti tai dynaamisesti ohjelmoida SDN-hallintaohjelmiston avulla. Se määrittelee lisäksi miten liikenteen kuuluu kulkea verkkolaitteissa, perustuen parametreihin kuten käyttömallit, sovellukset ja pilvipalvelun resurssit. Koska OpenFlow sallii verkon ohjelmoinnin yksittäisen liikennevuon mukaan, se tarjoaa hyvin hajautetunkin järjestelmän kontrollin. Tämän vuoksi verkko kykenee vastaamaan sovellusten, käyttäjän ja istuntotasojen mukaisiin vaatimuksiin reaaliajassa. Nykyinen IP-pohjainen reititys ei tarjoa tämänkaltaista hallintaa, sillä kaikkien liikennevoiden on kuljettava samaa reittiä kahden päätepisteen välillä, riippumatta päätepisteiden erilaisista vaatimuksista.

OpenFlow on avaintekijä SDN-arkkitehtuurin mahdollistamisessa ja se on tällä hetkellä ainoa standardisoitu SDN-protokolla joka sallii aikaisemmin esitetyn hallintakerroksen ja datakerroksen suoran manipuloinnin. Vaikka alun perin OpenFlowta käytettiin vain Ethernet-pohjaisten verkkojen kanssa, OpenFlowta voidaan käyttää myös paljon laajemmissa tapauksissa. OpenFlow-perusteista SDN-arkkitehtuuria voidaan käyttää jo olemassa olevissa virtuaalisissa ja fyysisissä verkoissa. Verkkolaitteet voivat tukea OpenFlow-perusteista eteenpäinohjausta yhtä hyvin kuin perinteistä eteenpäinohjausta, mikä tekee OpenFlowsta yrityksille ja palveluntarjoajille sen käyttöönoton todella helpoksi jopa usean eri laitevalmistajan laitteilla muodostetussa verkossa.

6.3 Toiminnallisuus

SDN:n tavoitteena on siis yksinkertaistaa verkon luomista ja hallintaa erottamalla sen data- ja ohjauskerros toisistaan ja luomalla yhteinen hallinta kaikille verkon laitteille niiden eteenpäinohjaus- ja reitityssääntöjen myötä. Erotuksella tarkoitetaan fyysistä erottamista eli datakerroksen ollessa fyysinen verkko voi ohjauskerros olla fyysisesti missä sijainnissa tahansa. SDN-konseptin tavoitteena on tehdä verkosta dynaaminen, hallittava, kustannustehokas ja sovellettava jolloin se olisi ideaalinen nykyisille sovel-

luksille, jotka vaativat suurta tiedonsiirtonopeutta ja dynaamisuutta. SDN:n tapauksessa kustannustehokkuudella tarkoitetaan sitä, että itse fyysinen verkko voi olla jo olemassa oleva vanha verkko. SDN on siis tavallaan rajapinta, jolla vanhasta fyysisestä verkosta saadaan suurempi hyöty ilman vanhojen investointien hylkäämistä.

SDN:n tärkeimmät ominaisuudet ja tavoitteet ovat: keskitetty hallinta eri laitevalmistajien ympäristöille, yksinkertaistettu automatisointi ja hallinta, mahdollisuus tehokkaaseen innovointiin, parannettu verkon luotettavuus ja tietoturva, hajautetumpi verkon hallinta ja parempi loppukäyttäjien käyttökokemus.

Keskitetty hallinta sinänsä ei ole uusi asia, sillä nykyiset fyysiset verkkolaitteet voidaan konfiguroida etäyhteydellä käyttäen yhtä etäpistettä, jolloin ei ole tarvetta mennä fyysisesti verkkolaitteen viereen. SDN:n tapauksessa kuitenkin keskitetyllä hallinnalla tarkoitetaan hieman laajempaa hallintaa, sillä sen avulla on mahdollista hallinnoida keskitetysti eri laitevalmistajien verkkolaitteita ja vielä samanaikaisesti. Näihin verkkolaitteisiin kuuluvat kytkimet, reitittimet ja virtuaaliset kytkimet. Keskitetty hallinta poistaa siis eri valmistajien tekemien laiteryhmien erillisen konfiguroinnin tarpeen ja ylläpitäjät voivat SDN-perusteisen organisoinnin ja hallinnan avulla nopeasti käyttöönottaa, konfiguroida ja päivittää laitteita koko verkon alueella.

SDN tarjoaa myös joustavan verkon automatisoinnin ja hallinnan ohjelmointimallin, joka mahdollistaa erilaisten automaattisten toimintojen luomisen niiden toimintojen tilalle, jotka nykyään tehdään manuaalisesti. Nämä automatisoinnin työkalut vähentävät toistuvaa työtä, verkon konfiguraatiovirheitä ja tukevat palveluperustaista toimintatapaa. Lisäksi SDN:n avulla pilvipalveluihin perustuvia sovelluksia voidaan hallita älykkäiden organisointi- ja provisiointijärjestelmien avulla, mikä pienentää myös toistuvaa työtä palveluntarjoajan kannalta. Näiden toimintojen avulla mahdollistetaan siis yksinkertaistettu automatisointi ja hallinta.

Mahdollisuus tehokkaaseen innovointiin saavutetaan ohjelmoitavuuden avulla. SDN:n avulla verkko voidaan ohjelmoida ja uudelleenohjelmoida reaaliaikaisesti vastaamaan juuri tiettyjä liiketoimintaan liittyviä vaatimuksia tai käyttäjävaatimuksia. Virtualisoimalla verkon infrastruktuurin ja erottamalla sen yksittäisistä verkkopalveluista esimerkiksi SDN ja OpenFlow antavat palveluntarjoajille ja jopa käyttäjille kyvyn muokata verkon käyttäytymistä ja käyttöönottaa uusia palveluita ja verkko-ominaisuuksia jopa tuntien sisällä.

SDN mahdollistaa ylläpitäjien määritellä korkean tason konfiguraatioita ja sääntöjä, jotka sitten siirtyvät infrastruktuuriin OpenFlow:n avulla. OpenFlow:n arkkitehtuuri poistaa tarpeen konfiguroida jokaista verkkolaitetta erikseen aina kun palvelu tai sovellus siirretään toiseen paikkaan tai sääntö muuttuu, mikä vähentää konfiguraatiovirheistä tai sääntöjen epämääräisyydestä johtuvia verkkovirheitä. Koska SDN-kontrollerit tarjoavat täyden näkyvyyden ja kontrollin verkosta, ne voivat varmistaa, että pääsynhallinta, liikenteen muokkaaminen, palvelun laatu (Quality of Service), turvallisuus ja muut säännöt ovat voimassa jatkuvasti langallisissa ja langattomissa verkkoinfrastruktuureissa, joihin voivat kuulua esimerkiksi sivutoimipisteet, kampukset tai datakeskukset. Organisaatiot ja palveluntarjoajat taas hyötyvät pienemmistä operaatiivisen toimin-

nan kustannuksista, dynaamisemmista konfigurointimahdollisuuksista, vähemmistä virheistä ja jatkuvasta konfiguroinnin ja sääntöjen varmistamisesta.

Hajautetumpi verkon kontrollointi on myös mahdollista SDN:n avulla. Tällä tarkoitetaan sitä, että OpenFlow:n avulla on mahdollista luoda sääntöjä hyvin hajautetusti, kuten istunto-, sovellus-, käyttäjä-, laite- tai sovellustasolla. Tämä voidaan lisäksi tehdä hyvin abstraktoidulla ja automatisoidulla tavalla. Tämä kontrolli antaa pilvipalveluntarjoajille mahdollisuuden tukea monikäyttäjyyttä (multitenancy), eli sitä että useat laitteet käyttävät yhdellä palvelimella suoritettavaa ohjelmistoa, poistamatta käytöstä liikenteen erottelua, turvallisuutta tai joustavaa resurssien hallintaa kun asiakkaat jakavat saman infrastruktuurin.

Keskittämällä verkon hallinnan ja tekemällä suoritustilan tiedon avoimeksi korkean tason sovelluksille, SDN-infrastruktuuri pystyy paremmin mukautumaan dynaamisiin käyttäjän tarpeisiin. Esimerkiksi palveluntarjoaja voisi tarjota lisämaksusta käyttäjilleen videopalvelun, jonka avulla käyttäjä saa parhaan mahdollisen videoresoluution automaattisesti ja ilman, että käyttäjä huomaa sitä. Nykyään käyttäjien tulee valita videon resoluutio erikseen ja sen toimivuudesta ei ole takeita verkon kannalta. Tämä taas johtaa viiveisiin ja katkoksiin, jotka huonontavat asiakkaan käyttökokemusta. OpenFlow:n avulla videosovellus pystyy tunnistamaan vapaana olevan kaistanleveyden reaaliajassa ja säätää videon resoluution automaattisesti sen mukaan. [74]

6.4 VMwaren ja Ciscon SDN-ratkaisut

Myös VMware ja Cisco ovat lähteneet kehittämään SDN-konseptiin perustuvaa ohjelmoitavaa verkkoarkkitehtuuria. VMware NSX on verkon virtualisoinnin alusta, joka tarjoaa tietokoneiden virtualisointia vastaavan toiminnon myös verkoille. VMware NSX:n tavoite on nopeuttaa verkon provisiointi päivistä sekunteihin, saavuttaa toiminnallista tehokkuutta automaation kautta ja mahdollistaa työkuormien siirto paikasta toiseen välittämättä fyysisen verkon topologiasta. Ciscon ACI (Application Centric Infrastructure) taas on arkkitehtuuri, jonka tavoitteena on radikaalisti yksinkertaistaa, optimoida ja kiihdyttää koko sovelluksen käyttöönottosykliä.

6.4.1 VMware NSX

VMware NSX:n avulla voidaan luoda ohjelmallisesti oleellisia verkon elementtejä erillään fyysisen verkon topologiasta. Sillä voidaan luoda esimerkiksi loogisia kytkimiä, reitittimiä, palomuureja, kuorman tasapainotukseen käytettäviä elementtejä ja VPN-toimintoja. Käyttäjät voivat lisäksi luoda eristettyjä verkkoja edellä mainittujen verkkokomponenttien erilaisista yhdistelmistä. Kuten SDN-konseptissa on ideana, myös VMware NSX voidaan ottaa käyttöön jo olemassa olevan fyysisen verkkoinfrastruktuurin kanssa.

Erityisesti VMware NSX -tuote sopii datakeskuksen automatisointiin, itse ylläpidettyyn yrityksen IT-infrastruktuuriin ja monikäyttäjyyttä hyödyntäviin pilviratkaisuihin. Sen avulla voidaan nopeuttaa verkon provisiointia, yksinkertaistaa virtuaalisten ja

fyysisten palveluiden käyttöönottoa ja asennusta sekä selkeyttää DMZ-muutoksia. DMZ eli demilitarized zone on ominaisuus, jonka avulla tietty alue verkosta voidaan asettaa niin, että siihen on suora pääsy kenellä tahansa. Tämä tarkoittaa sitä, että esimerkiksi verkkoon hyökkäävä osapuoli pääsee DMZ:n osoitealueella oleviin verkkolaitteisiin, mutta ei muihin. DMZ:aa voidaan käyttää myös, mikäli tietylle verkon laitteelle halutaan saada mahdollisimman suora pääsy verkkoon ilman, että palomuurit tai muut säännöt reitittimessä tai kytkimessä estävät sitä. VMware NSX sopii myös yrityksille, jotka ylläpitävät itse IT-infrastruktuuriaan, sillä se mahdollistaa sovellusten nopean käyttöönoton ja automatisoidun verkon ja palveluiden provisioinnin yksityisille pilville ja testisekä kehitysympäristöille. Se mahdollistaa lisäksi eristetyt testaus-, kehitys- ja tuotantoympäristöt samassa fyysisessä infrastruktuurissa. VMware NSX sopii myös monikäyttäjyyttä hyödyntäviin pilviratkaisuihin, sillä sen avulla voidaan verkon provisointi sen käyttäjille automatisoida ja lisäksi käyttäjät pysyvät täysin eristyksissä toisistaan. Lisäksi VMware NSX maksimoi fyysisten resurssien jakamisen käyttäjien kesken. [75]

VMware NSX toimii siis suurelta osin SDN-konseptin määrittämillä tavoilla. Se käyttää API-rajapintoja sovellusten ja oman hallintaohjelmistonsa välillä ja se käyttää overlay-teknologiaa hallintaohjelmiston ja verkkoinfrastruktuurin välillä. Erona kuitenkin on, että VMware NSX pystyy käyttämään OpenFlow-teknologian lisäksi myös muita overlay-teknologioita eli esimerkiksi VXLANia. [76]

6.4.2 Cisco ACI

VMwaren lisäksi Cisco on mukana SDN-konseptiin perustuvassa tuotekilpailussa. Cisco ACI (Application Centric Infrastructure) on VMware NSX:ää vastaava, SDN-konseptia hyödyntävä tuote. Cisco ACI perustuu myös suurilta osin SDN-konseptin pääperiaatteisiin. VMware NSX ja Cisco ACI eroavat kuitenkin jonkin verran toisistaan, sillä VMware ylistää NSX:n hyvää virtuaalisten kytkinten toiminnallisuutta erottaen verkon ja hallinnan toisistaan overlay-teknologian avulla, mutta Cisco ACI sulauttaa enemmänkin rauta-alustan ja ohjelmistot sääntöjen perusteella toimivaksi verkkoinfrastruktuuriksi, joka määritellään tiettyjen sovellusten tarpeiden mukaisesti. [77]

Cisco ACI käyttää kokonaisvaltaista järjestelmäpohjaista lähestymistapaa, jossa se integroi tiukasti yhteen fyysiset ja virtuaaliset elementit, avoimen ekosysteemimallin, innovaatioita tukevat sovelluskohtaiset integroidut piirit eli ASICsit (Application-specific integrated circuits), rauta-laitteiston ja ohjelmiston. Ciscon lähestymistapa SDN:ään on uniikki ja se käyttää yleisiä sääntöihin perustuvia toimintamalleja ACI-valmiiden verkkojen ja turvallisuuskomponenttien, kuten laskennan ja levytilajärjestelmien välillä. Näiden avulla Cisco ACI pystyy merkittävästi vähentämään monimutkaisuutta ja kustannuksia verrattuna perinteiseen verkkoarkkitehtuuriin.

Cisco haluaa ACI:n avulla ratkaista ongelmia datakeskusten malleissa, joissa pilvipalvelut, mobiililiikkuvuus ja big data-sovellukset aiheuttavat muutoksia perinteisiin tarpeisiin. Infrastruktuurin tulee olla jatkossa sovellustietoisempi ja ketterämpi, tukeakseen dynaamista sovellusten lisäämistä ja poistoa. Uusien ei-virtuaalisten sovellusten uusi tuleminen tarkoittaa, että infrastruktuurin pitää tukea fyysistä, virtuaalista ja

pilven integrointia säilyttäen samalla täysi näkyvyys infrastruktuurista. Ciscon ACI mahdollistaa myös infrastruktuurista riippuvaisten sovellusten käyttävän datakeskuksen dynaamisesti jaettuja resursseja. Lisäksi skaalautumismallit vaativat nykyään poikittaista liikennöintiä esimerkiksi palvelimien välillä, mikä vaatii parempaa verkon suorituskykyä ja skaalautuvuutta. Useammasta pilvestä koostuvat verkkoratkaisut vaativat lisäksi, että infrastruktuuri on tietoturvallinen ja tietoinen monikäyttäjyydestä.

Ciscon tapauksessa looginen topologia on SDN-konseptin mukainen. Suurimpana erona ja samalla tärkeimpänä Cisco ACI:n komponenttina on APIC (Application Policy Infrastructure Controller). Sen tehtävänä on toimia hallintaohjelmistona sovelluskerroksen ja verkkoinfrastruktuurin datakerroksen kanssa. Ciscon ACI toimii VMwaren tavoin kaikissa isäntälaitteistoissa, oli sitten kyseessä esimerkiksi ESXi-hypervisor, Microsoft Hypervisor tai Red Hat -hypervisor. [78]

Cisco ACI:n tapauksessa on ymmärrettävä, että vaikka se on SDN-konseptiin perustuva, se ei käytä hyväkseen OpenFlow-protokollaa. Cisco korvaa OpenFlow:n käytön nimenomaan sillä, että se on sovellusorientoitunut verkko-orientoituneisuuden sijaan. Näin ollen APIC-ohjain siis ohjaa kaikkia verkkolaitteita sen alla. Tämän perusteella voidaankin miettiä, onko Ciscon ACI todella SDN-teknologia vai onko se vaihtoehto sille. Joidenkin mielestä Cisco ACI on SDN:ään perustuva, mutta siitä pitemmälle kehitetty versio. SDN itsessäänhän on konsepti, jonka perusteella eri valmistajat tekevät omat ratkaisunsa, vaikka Open Network Foundation suosittelisikin mahdollisimman avoimien standardien käyttöä. [79]

7 YHTEENVETO

Tämän työn tarkoituksena oli esitellä ja tutkia pilvipalveluihin liittyviä virtualisoituja lähiverkkoja niiden komponentteja, tutustuttaa lukija SDN-konseptiin sekä vertailla mahdollisuuksia pilviympäristöjen eri valmistajien välillä. Työ tehtiin SSP Yhtiöt Oy:lle. Jotta työstä saatiin mahdollisimman kattava, valittiin tarkasteltavaksi kaksi suurinta kaupallista pilviympäristöjen valmistajaa, VMware ja Microsoft. Suurin paino työssä kohdistui virtuaalisten kytkinten toiminnallisuuteen ja verkon muihin komponentteihin kuten virtuaalisiin yhdyskäytäviin. Lisäksi työssä käsiteltiin VMwaren ja Microsoftin kehittämiä verkon virtualisointiin liittyviä overlay-teknologioita, VXLANia ja HVN:ää, koska niiden merkityksen ennustetaan verkon virtualisoinnin kannalta olevan suuri. Jotta työ ei olisi muodostunut pelkästään kaupallisista tuotteista, otettiin lyhyesti tarkasteluun myös avoimeen lähdekoodiin perustuva, ilmainen Open vSwitch. Työn edetessä haluttiin myös todentaa pilvipalvelun redundanttisuuteen liittyviä ominaisuuksia lähiverkon kannalta, jotta nämä ominaisuudet eivät jäisi ainoastaan valmistajien myyntipuheiksi. Lähiverkon redundanttisuuden testaaminen suoritettiin SSP Yhtiöt Oy:n VMware-pilviympäristössä. Työn lisätavoitteena oli työn tekijän perehdyttäminen pilvipalveluiden toiminnallisuuteen ja mahdollisuuksiin. Työn aineistona käytettiin pääasiassa valmistajien tuotedokumentaatioita ja kyseiseen aiheeseen liittyviä Internet-lähteitä, kuten blogeja, artikkeleita ja konfigurointiohjeita.

Microsoft ja VMware ovat IaaS-pilviympäristöjen edelläkävijöitä. Ensimmäinen Hyper-V isäntäpalvelinohjelmisto julkaistiin vuonna 2008 ja VMwaren ESX jo vuonna 2001. Microsoftin voidaan siis sanoa tulleen markkinoille jonkin verran myöhemmin kuin VMwaren. Microsoftin ja VMwaren voidaan sanoa olevan lähes samalla tasolla lähiverkon toiminnallisuuden ja verkon virtualisoinnin kannalta. Microsoftin lähestymistapa verkon virtualisointiin ja virtualisoituihin kytkimiin on enemmän sovelluskeskittynyt kuin VMwaren. VMware keskittyy enemmän laitteistoihin ja niiden toiminnan takaamiseen. Microsoft on myös ajatellut lähiverkon kytkimissä laajennettavuutta kolmannen osapuolen tuotteilla. VMwaren lähestymistapa on enemmänkin suljettu ympäristö. Suljetulla ympäristöllä voidaan sanoa olevan omat puolensa, sillä sen toiminta pysyy muuttumattomana ja vianrajaus helpottuu. Microsoftin laajennettavuudet mahdollistavat kuitenkin toiminnallisuuden kehittämisen jakamisen koko yhteisölle, mikä joissakin tilanteissa saattaa antaa kilpailuedun markkinoilla. Tästä esimerkkinä SDN-konseptiin kuuluvan OpenFlow-protokollan tuki Microsoftin virtuaaliselle kytkimelle.

Verkon virtualisoinnin kannalta VMware ja Microsoft ovat hyvin lähellä toistensa toteutuksia. VMwaren VXLAN ja Microsoftin HVN muistuttavat toiminnallisuudeltaan todella paljon toisiaan. Käytännössä Microsoftin HVN:n NVGRE-protokollan

käyttö on tuettu paremmin nykyisissä fyysisen verkon laitteissa, joten se antaa Microsoftille kilpailuetua. VMwaren VXLAN on kuitenkin joillakin toiminnallisuuksillaan edellä Microsoftia. Tästä esimerkkinä kuormantasaus porttikohtaisesti, mikä tasoittaa verkon kuormitusta. VXLANin ja HNV:n kannalta Microsoft ja VMware ovat lähemmässä tarkastelussa ja tavoitteissaan niin lähellä toisiaan, että niiden kannattaisi ehkä jopa harkita yhteistyön tekemistä, jotta verkon virtualisoinnista saataisiin mahdollisimman yhdenmukainen standardi.

SDN-konsepti käsiteltiin työssä omana lukunaan, sillä se on Open Network Foundationin kehittämä avoimeen lähdekoodiin perustuva konsepti. SDN on konseptina selkeä ja sen tavoitteet ovat koko tietoliikennealaa hyödyttävät. Tavoitteena on luoda yhdenmukainen standardi verkon virtualisointia koskien. Tavoitteet ovat selkeät ja hyvät, mutta kovan kilpailun vuoksi saattaa olla vaikeata luoda avoimesti levitettäviä ratkaisuja koko alan laajuudelle. Microsoft ja VMware esimerkiksi ovat miljardiluokan liikevaihdolla toimivia yrityksiä ja kuten yritysten tavoitteena on, ne yrittävät tuottaa mahdollisimman paljon liikevoittoa omistajilleen. Tämän vuoksi avoimeen lähdekoodiin perustuvan standardin luominen isojen kilpailevien yritysten välille saattaa osoittautua vaikeaksi. Tämä ei kuitenkaan välttämättä tarkoita epäonnistumista, sillä kuten edellä mainittiin, Microsoft tukee SDN-konseptin OpenFlow-protokollaa virtuaalisessa kytkimessään ja tämä saattaa tehdä muutoksen myös VMwaren ajatteluun SDN-konseptista.

VMware ja Microsoft tarjoavat pilviympäristöratkaisuissaan todella paljon toiminnallisuuksia niin verkon, tietokoneiden virtualisoinnin kuin myös lisäominaisuuksien kannalta. On kuitenkin tärkeää ottaa huomioon, että virtualisointi, varsinkin verkkojen osalta, vaatii useita erilaisia komponentteja toimiakseen ja niiden toimivuudesta ja tehokkuudesta ei voi olla varma ennen kuin sitä käytännössä testataan. Lisäksi vaatimukset erilaisille asetuksille ja määrityksille saattavat aiheuttaa käyttöönotossa ongelmia, sillä keskitetyn hallinnan ohjelmistot ovat suhteellisen uusia ja kaikkia virheitä, joita käyttäjä niissä tekee, ei välttämättä huomioida.

Lisäksi hieman valmistajasta riippuen, ovat ratkaisut edelleen hyvin sidottuja alla olevaan fyysiseen laitteistoon ja pilviympäristön valmistajaan, jolloin yksinkertaisesta ja palveluperusteisesta pilvipalvelusta saattaakin muodostua sen hankkijalle suuremmat investoinnit kuin annetaan ymmärtää. SDN-konseptin voidaan sanoa olevan näkökulma oikeaan suuntaa, sillä sen laajempi käyttöönotto ja hyväksyntä mahdollistaisivat laitevalmistajasta riippumaton ratkaisun verkon virtualisoinnille.

Työ onnistui tavoitteissaan hyvin. Aineistojen helppo saatavuus molempien isojen valmistajien dokumentaatioista oli huomattava etu työtä tehdessä ja lisäksi SSP Yhtiöt Oy tarjosi pääsyn VMwarella toteutettuun pilviympäristöön, jotta toiminnallisuuksia pääsi kokeilemaan käytännössä. Tämä antoi lisäperspektiiviä ja myös kriittisyyttä valmistajien omien dokumentointien lukemiseen. Työn aihe oli itsessään ihan uutta asiaa työn tekijälle, mikä vaati paljon opiskelua aiheeseen liittyen, mutta samalla se antoi takaisin yhtä paljon.

LÄHTEET

[1] Haydin, V. Dive into the cloud: brief technology introduction. Eleks research & development blog [WWW]. 2012.[Viitattu 3.3.2014]. Saatavissa: http://www.elekslabs.com/2012/12/dive-into-cloud-brief-technology.html

[2] Salo, I. Cloud computing - palvelut verkossa. Porvoo 2010, WSOYpro Oy. 168 p.

[3] Salesforce.com. Why Move to the Cloud? 10 Benefits of Cloud Computing. Salesforce.com [WWW]. 2014. [Viitattu 3.3.2014]. Saatavissa: http://www.salesforce.com/uk/socialsuccess/cloud-computing/why-move-to-cloud-10-benefits-cloud-computing.jsp

[4] Mell, P. & Grance, T. The NIST Definition of Cloud Computing. U.S. Department of Commerce [WWW]. 2011. [Viitattu 3.3.2014]. Saatavissa: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[5] Hurwitz, J., Kaufman, M., Halper, F. & Kirsch, D. Exploring Types of PaaS Environments in Cloud Computing [WWW]. 2012. [Viitattu 3.3.2014]. Saatavissa: http://www.dummies.com/how-to/content/exploring-types-of-paas-environments-in-cloud-comp.html

[6] Hurwitz, J., Bloor, R., Kaufman, M. & Halper, F. Examining the Types of SaaS Platforms in Cloud Computing [WWW]. 2012. [Viitattu 3.3.2014]. Saatavissa: http://www.dummies.com/how-to/content/examining-the-types-of-saas-platforms-in-cloud-com.html

[7] Popek, G.J & Goldberg, R.P. Formal Requirements for Virtualizable Third Generation Architectures. Communications of the ACM. 17(1974)7. Pp. 412-421.

[8] Rouse, M. & Madden, J. Desktop virtualization [WWW]. 2011. [Viitattu 3.3.2014]. Saatavissa: http://searchvirtualdesktop.techtarget.com/definition/desktop-virtualization

[9] Cisco. Network Considerations to Optimize Virtual Desktop Deployment [WWW]. 2009. [Viitattu 3.3.2014]. Saatavissa: http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-4500-series-switches/white_paper_c11-531553.pdf

[10] Dropbox. Where does Dropbox store everyone's data? [WWW]. [Viitattu 3.3.2014]. Saatavissa: https://www.dropbox.com/help/7/en

[11] StarWind Software. Starwind's Shared Storage for VMware vSphere, VMware ESX and ESXi [WWW]. [Viitattu 3.3.2014]. Saatavissa: http://esx.starwindsoftware.com/

[12] Oracle. Overview of Network Virtualization [WWW]. 2012. [Viitattu 3.3.2014]. Saatavissa: http://docs.oracle.com/cd/E26502_01/html/E28992/gfkbw.html

[13] Linkedin. VMware - Overview [WWW]. [Viitattu 3.3.2014]. Saatavissa: http://www.linkedin.com/company/vmware

[14] Microsoft. Windows Server 2012 R2 [WWW]. [Viitattu 3.3.2014]. Saatavissa: http://www.microsoft.com/en-us/server-cloud/products/windows-server-2012-r2/default.aspx#fbid=vH02zhP861p

[15] Linux-KVM. Kernel Based Virtual Machine [WWW]. [Viitattu 3.3.2014]. Saatavissa: http://www.linux-kvm.org/page/Main_Page

[16] Citrix. XenServer - Industry leading open-source server virtualization [WWW]. [Viitattu 3.3.2014]. Saatavissa: http://www.citrix.com/products/xenserver/overview.html

[17] VMware. vCloud Director User's Guide [WWW]. 2011. [Viitattu 3.3.2014]. Saatavissa: http://www.vmware.com/pdf/vcd_15_users_guide.pdf

[18] VMware. Virtual Networking Concepts [WWW]. 2007. [Viitattu 3.3.2014]. Saatavissa: http://www.VMware.com/files/pdf/virtual_networking_concepts.pdf

[19] Brunsdon, G. What vnic? Choosing an adapter for your VM [WWW]. 2009. [Viitattu 3.3.2014]. Saatavissa: http://blogs.VMware.com/vsphere/2009/06/what-vnic-choosing-an-adapter-for-your-vm.html

[20] Brunsdon, G. Virtual Switches vs Physical Switches plus more on "Let's Talk Security..." [WWW]. 2009. [Viitattu 3.3.2014]. Saatavissa: http://blogs.VMware.com/vsphere/2009/06/virtual-switches-vs-physical-switches-plus-more-on-lets-talk-security.html

[21] Cisco. Inter-Switch Link and IEEE 802.1Q Frame Format [WWW]. 2006. [Viitattu 3.3.2014]. Saatavissa: http://www.cisco.com/c/en/us/support/docs/lan-switching/8021q/17056-741-4.pdf

[22] VMware. Load Based Teaming in VMware ESX 4.x and VMware ESXi 4.x [WWW]. 2013. [Viitattu 3.3.2014]. Saatavissa: http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1022590

[23] VMware. VMware vNetwork Distributed Switch: Migration and Configuration [WWW]. 2009. [Viitattu 3.3.2014]. Saatavissa: http://www.vmware.com/files/pdf/vsphere-vnetwork-ds-migration-configuration-wp.pdf

[24] VMware. Overview of vNetwork Distributed Switch concepts [WWW]. [Viitattu 3.3.2014]. Saatavissa: http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1010555

[25] LucD notes. dvSwitch scripting - Part 9 - Traffic Shaping [WWW]. 2011. [Viitattu 3.3.2014]. Saatavissa: http://www.lucd.info/2011/06/11/dvswitch-scripting-part-9-traffic-shaping/

[26] VMware. Private VLANs [WWW]. [Viitattu 3.3.2014]. Saatavissa: http://pubs.vmware.com/vsphere-51/index.jsp?topic=%2Fcom.vmware.vsphere.networking.doc%2FGUID-A9287D46-FDE0-4D64-9348-3905FEAC7FAE.html

[27] Wahl, C. Understanding vSphere Private VLANs For Fun and Profit [WWW]. 2012. [Viitattu 3.3.2014]. Saatavissa: http://wahlnetwork.com/2012/05/14/understanding-vsphere-private-vlans-for-fun-and-profit/

[28] Ewald, M. PVLAN - A Widely Underutilized Feature [WWW]. 2012. [Viitattu 3.3.2014]. Saatavissa: http://www.vxpertise.net/2012/11/pvlan-a-widely-underutilized-feature/

[29] VMware. What's New in VMware vSphere 5.1 - Networking [WWW]. 2012. [Viitattu 3.3.2014]. Saatavissa: http://www.vmware.com/files/pdf/techpaper/Whats-New-VMware-vSphere-51-Network-Technical-Whitepaper.pdf

[30] Epping, D. dvSwitch? [WWW]. 2009. [Viitattu 3.3.2014]. Saatavissa: http://www.yellow-bricks.com/2009/09/24/dvswitch/

[31] Herrod, S. Towards Virtualized Networking for the Cloud [WWW]. 2011. [Viitattu 3.3.2014]. Saatavissa: http://blogs.vmware.com/vmware/2011/08/towards-virtualized-networking-for-the-cloud.html

[32] Mahalingam, M., Dutt, D., Duda, K., Agarwal, P., Kreeger, L., Sridhar, T., Bursell, M. & Wright, C. VXLAN: A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks [standardin luonnos]. 2012. [Viitattu 3.3.2014]. Saatavissa: http://tools.ietf.org/id/draft-mahalingam-dutt-dcops-vxlan-08.txt

[33] VMware. VXLAN - What it is, Components that Make it Work, and Benefits [WWW]. 2013. [Viitattu 3.3.2014]. Saatavissa: https://blogs.vmware.com/smb/2013/09/vxlan-what-it-is-components-that-make-it-work-and-benefits.html

[34] VMware. VXLAN-Backed Considerations [WWW]. [Viitattu 3.3.2014]. Saatavissa: http://download3.vmware.com/vcat/documentation-center/index.html#page/Architecting%20a%20vCloud/3a%20Architecting%20a%20VMware%20vCloud.2.063.html

[35] Epping, D. VXLAN requirements [WWW]. 2012. [Viitattu 3.3.2014]. Saatavissa: http://www.yellow-bricks.com/2012/10/04/vxlan-requirements/

[36] Fitzhugh, R. vCloud Director 5.1 Networking Concepts [WWW]. 2013. [Viitattu 3.3.2014]. Saatavissa: http://www.globalknowledge.co.uk/content/files/documents/640774/640807/vcloud-director-5.1-networking-concepts

[37] VMware. VMware vShield Edge and vShield App Reference Design Guide [WWW]. 2010. [Viitattu 3.3.2014]. Saatavissa: http://www.vmware.com/files/pdf/techpaper/vShield-design-guide.pdf?rct=j&q=&esrc=s&source=web&cd=2&ved=0CDAQFjAB&url=https://www.vmware.com/go/vshield-design-guide&ei=iRn6UsfkC6WE4ASHp4DwDA&usg=AFQjCNExM9M4_3lGP2jGit1TBaATeS4z6Q&sig2=szzxnNFfmj9sgWW08Q6buA

[38] Microsoft. Unified management for the Cloud OS - System Center 2012 R2 [WWW]. 2013. [Viitattu 3.3.2014]. Saatavissa: http://download.microsoft.com/download/7/7/2/7721670F-DEF0-40D3-9771-43146DED5132/System_Center_2012%20R2_Overview_White_Paper.pdf

[39] Microsoft. Hyper-V Virtual Switch Overview [WWW]. 2013. [Viitattu 3.3.2014]. Saatavissa: http://technet.microsoft.com/en-us/library/hh831823.aspx

[40] Microsoft. Validation Ports [WWW]. [Viitattu 3.3.2014]. Saatavissa: http://msdn.microsoft.com/en-us/library/windows/hardware/hh582275(v=vs.85).aspx

[41] Microsoft. Operational Ports [WWW]. [Viitattu 3.3.2014]. Saatavissa: http://msdn.microsoft.com/en-us/library/windows/hardware/hh582267(v=vs.85).aspx

[42] Microsoft. External Network Adapters [WWW]. [Viitattu 3.3.2014]. Saatavissa: http://msdn.microsoft.com/en-us/library/windows/hardware/hh582256(v=vs.85).aspx

[43] Microsoft. Types of Physical Network Adapter Configurations [WWW]. [Viitattu 3.3.2014]. Saatavissa: http://msdn.microsoft.com/en-us/library/windows/hardware/hh582274(v=vs.85).aspx

[44] Microsoft. Internal Network Adapters [WWW]. [Viitattu 3.3.2014]. Saatavissa: http://msdn.microsoft.com/en-us/library/windows/hardware/hh582260(v=vs.85).aspx

[45] Microsoft. Virtual Machine Network Adapters [WWW]. [Viitattu 3.3.2014]. Saatavissa: http://msdn.microsoft.com/en-us/library/windows/hardware/hh598304(v=vs.85).aspx

[46] Microsoft. Packet Flow through the Extensible Switch Data Path [WWW]. [Viitattu 3.3.2014]. Saatavissa: http://msdn.microsoft.com/en-us/library/windows/hardware/hh582269(v=vs.85).aspx

[47] Microsoft. Hyper-V Extensible Switch Control Path for OID Requests [WWW]. [Viitattu 3.3.2014]. Saatavissa: http://msdn.microsoft.com/en-us/library/windows/hardware/hh598166(v=vs.85).aspx

[48] Microsoft. Hyper-V Extensible Switch Control Path for NDIS Status Indications [WWW]. [Viitattu 3.3.2014]. Saatavissa: http://msdn.microsoft.com/en-us/library/windows/hardware/hh598165(v=vs.85).aspx

[49] Microsoft. Hyper-V Extensible Switch Save and Restore Operations [WWW]. [Viitattu 3.3.2014]. Saatavissa:http://msdn.microsoft.com/en-us/library/windows/hardware/hh598184(v=vs.85).aspx

[50] Microsoft. Create Security Policies with Extended Port Access Control Lists for Windows Server 2012 R2 [WWW]. [Viitattu 3.3.2014]. Saatavissa: http://technet.microsoft.com/en-us/library/dn375962.aspx

[51] 5nine Software. 5nine Cloud Security 4.0 for Hyper-V [WWW]. [Viitattu 3.3.2014]. Saatavissa: http://www.5nine.com/5nine-security-for-hyper-v-product.aspx

[52] Finn, A. Windows Firewall On Hyper-V Management OS (Host) Has Nothing To Do With Virtual Machines[WWW]. 2013. [Viitattu 3.3.2014]. Saatavissa: http://www.aidanfinn.com/?p=15222

[53] Microsoft. NIC Teaming Overview [WWW]. 2012. [Viitattu 3.3.2014]. Saatavissa: http://technet.microsoft.com/library/hh831648.aspx

[54] Microsoft. RRAS and DHCP [WWW]. 2012. [Viitattu 3.3.2014]. Saatavissa: http://technet.microsoft.com/en-us/library/dd458962(v=ws.10).aspx

[55] Siron, E. Hyper-V Virtual Switch Explained, Part 2 [WWW]. 2013. [Viitattu 3.3.2014]. Saatavissa: http://www.altaro.com/hyper-v/hyper-v-virtual-switch-explained-part-2/

[56] NEC. NEC Develops Extension Software Supporting OpenFlow for Windows Server 2012 Hyper-V Virtual Switches [WWW]. 2012. [Viitattu 3.3.2014]. Saatavissa: http://www.necam.com/about/read.cfm?press_id=cfe643de-b2ff-4266-bf8e-222921f730e9

[57] Microsoft. Hyper-V Network Virtualization Overview [WWW]. 2014. [Viitattu 3.3.2014]. Saatavissa: http://technet.microsoft.com/en-us/library/jj134230.aspx

[58] Sridharan, M., Duda, K., Ganga, I., Greenberg, A., Lin, G., Pearson, M., Thaler, P., Tumuluri, C., Venkataramiah, N. & Wang, Y. NVGRE: Network Virtualization using Generic Routing Encapsulation [standardin luonnos]. 2011. [Viitattu 3.3.2014]. Saatavissa: http://tools.ietf.org/id/draft-sridharan-virtualization-nvgre-04.txt

[59] Alila, A. Microsoft Hyper-V:n käyttöönotossa huomioitavat asiat ja parhaat käytännöt. Hyper-V verkon virtualisointi [WWW]. 2013. [Viitattu 3.3.2014]. Saatavissa: https://blogs.technet.com/b/fiitpro/archive/2013/11/21/microsoft-hyper-v-n-k-228-ytt-246-246-notossa-huomioitavat-asiat-ja-parhaat-k-228-yt-228-nn-246-t-hyper-v-verkon-virtualisointi.aspx

[60] Microsoft. Windows Server Gateway [WWW]. 2013. [Viitattu 3.3.2014]. Saatavissa: http://technet.microsoft.com/en-us/library/dn313101.aspx

[61] Open vSwitch. Overview of functionality and components [WWW]. [Viitattu 3.3.2014]. Saatavissa: http://git.openvswitch.org/cgi-bin/gitweb.cgi?p=openvswitch;a=blob_plain;f=README;hb=HEAD

[62] Project Floodlight. Floodlight Is an Open SDN Controller [WWW]. 2014. [Viitattu 3.3.2014]. Saatavissa: http://www.projectfloodlight.org/floodlight/

[63] Open vSwitch. How to Use Open vSwitch with Libvir [WWW]. [Viitattu 3.3.2014]. Saatavissa: http://git.openvswitch.org/cgi-bin/gitweb.cgi?p=openvswitch;a=blob_plain;f=INSTALL.Libvirt;hb=HEAD

[64] Spenneberg, R. Virtual switching with Open vSwitch - Switching Station [WWW]. [Viitattu 3.3.2014]. Saatavissa: http://www.admin-magazine.com/CloudAge/Articles/Virtual-switching-with-Open-vSwitch

[65] Dineley, D., Ferrill, P. Virtualization showdown: Microsoft Hyper-V 2012 vs. VMware vSphere 5.1 [WWW]. 2013. [Viitattu 3.3.2014]. Saatavissa: http://www.infoworld.com/d/virtualization/virtualization-showdown-microsoft-hyper-v-2012-vs-vmware-vsphere-51-217125

[66] VMware. Flawed Logic Behind Microsoft’s Virtualization and Private Cloud Cost Comparisons [WWW]. 2012. [Viitattu 3.3.2014]. Saatavissa: https://blogs.vmware.com/virtualreality/2012/11/flawed-logic-behind-microsofts-virtualization-and-private-cloud-cost-comparisons.html

[67] VMware. Total cost comparison summary: VMware vSphere vs. Microsoft Hyper-V [WWW]. 2012. [Viitattu 3.3.2014]. Saatavissa: http://www.vmware.com/files/include/microsite/sddc/principled_technologies_vmware_vs_microsoft_tco.pdf

[68] VMware. Configuration Maximums - VMware vSphere 5.5 [WWW]. 2013. [Viitattu 3.3.2014]. Saatavissa: http://www.vmware.com/pdf/vsphere5/r55/vsphere-55-configuration-maximums.pdf

[69] VMware. VMware VMotion [WWW]. 2009. [Viitattu 3.3.2014]. Saatavissa: http://www.vmware.com/files/pdf/VMware-VMotion-DS-EN.pdf

[70] VMware. vSphere vMotion Networking Requirements [WWW]. [Viitattu 3.3.2014]. Saatavissa: http://pubs.vmware.com/vsphere-51/index.jsp?topic=%2Fcom.vmware.vsphere.vcenterhost.doc%2FGUID-3B41119A-1276-404B-8BFB-A32409052449.html

[71] VMware. VMware High Availability [WWW]. 2009. [Viitattu 3.3.2014]. Saatavissa: http://www.vmware.com/files/pdf/VMware-High-Availability-DS-EN.pdf

[72] Engelen, N. VMWorld 2012: INF-BCO2655: VMware vSphere Fault Tolerance for Multiprocessor Virtual Machines [WWW]. 2012. [Viitattu 3.3.2014]. Saatavissa: http://foonet.be/2012/10/09/vmworld-2012-inf-bco2655-vmware-vsphere-fault-tolerance-for-multiprocessor-virtual-machines/

[73] VMware. VMware Fault Tolerance [WWW]. 2009. [Viitattu 3.3.2014]. Saatavissa: http://www.vmware.com/files/pdf/VMware-Fault-Tolerance-FT-DS-EN.pdf

[74] Open Networking Foundation. Software-Defined Networking: The New Norm for Networks [WWW]. 2012. [Viitattu 3.3.2014]. Saatavissa: https://www.opennetworking.org/images/stories/downloads/sdn-resources/white-papers/wp-sdn-newnorm.pdf

[75] VMware. VMware NSX [WWW]. 2013. [Viitattu 3.3.2014]. Saatavissa: http://www.vmware.com/files/pdf/products/nsx/VMware-NSX-Datasheet.pdf

[76] Kerner, S.M. VMware Debuts NSX for Network Virtualization [WWW]. 2013. [Viitattu 3.3.2014]. Saatavissa: http://www.enterprisenetworkingplanet.com/datacenter/vmware-debuts-nsx-for-network-virtualization.html

[77] Banks, E. SDN showdown: Examining the differences between VMware's NSX and Cisco's ACI [WWW]. 2014. [Viitattu 3.3.2014]. Saatavissa: http://www.networkworld.com/news/2014/010614-vmware-nsx-cisco-aci-277154.html?page=7

[78] Cisco. Cisco Application Centric Infrastructure [WWW]. 2013. [Viitattu 3.3.2014]. Saatavissa: http://www.cisco.com/c/dam/en/us/products/collateral/cloud-systems-management/aci-fabric-controller/at-a-glance-c45-729864.pdf

[79] Kinghorn, G. Is ACI Really SDN? One Point of View to Clarify the Conversation [WWW]. 2014. [Viitattu 3.3.2014]. Saatavissa: https://blogs.cisco.com/datacenter/is-aci-really-sdn-one-point-of-view-to-clarify-the-conversation/